LT Auditor+ 8.0 SP2 SQL Report Generator

User Guide

BLUE LANCE
COMPUTER SECURITY SOFTWARE

CONTACT INFORMATION

Blue Lance, Inc.
1700 West Loop South, Suite 1100
Houston, TX 77027
Phone number: 713-680-1187
Fax number: 713-622-1370
Web address: **http://www.BlueLance.com**

COPYRIGHT © 2002 Blue Lance, Inc.

Blue Lance, LT Auditor+ 8, and the Report Generator are registered trademarks of Blue Lance, Inc.

Microsoft, Windows 2000, Windows NT, Windows Advanced Server, SQL Server 2000 and SQL Server 7.0 are registered trademarks of Microsoft Corporation.

Novell and NetWare are registered trademarks of Novell, Inc.

Intel and Pentium are registered trademarks of Intel Corporation.

Oracle, Oracle8*i*, and Net8 are registered trademarks of Oracle Corporation.

Pervasive and Btrieve are trademarks of Pervasive Software Inc.

Blue Lance shall not be held accountable for technical or editorial errors within this document. This document is provided “as is” without warranty of any kind and is subject to change without notice.

Contents

Chapter 1 — Overview

Report Generator 1

Chapter 2 — Installing the Report Generator

Overview 1
Requirements 1
  Installing the Report Generator 2

Chapter 3 — Constructing a Database

Overview 1
Space Considerations 1
Constructing a SQL Database 2
  Creating a Basic Database 3
  Creating a Custom Database 6
  Creating Tables, Views, Stored Procedures, and Audit Triggers 10
  Creating Tables, Views, and Stored Procedures for Exchange Logs 10
  Creating Tables, Views, and Stored Procedures for Extended File System Logs 11
  Assigning Permissions to the Database 12
  Creating a Maintenance Plan for SQL Server 15
  Archiving the Database and Deleting Data 19
    Creating a Flat Database 19
    Deleting Data 29
Constructing an Oracle Database 33
  Oracle8*i* Configuration Notes 33
    Database and Instance Name Issues 33
    Java Option 33
  Oracle Net8 Configuration Notes 34
  Running Oracle Scripts 34
  Setting Up an Entry to the Tnsnames.ora File Using Net8 Assistant 35

Chapter 4 — Using the Report Generator

Overview 1
Using the Report Generator 1
Adding a New Data Source 2
Microsoft SQL Server 3
Oracle 4
Adding a New Report Group 5
Deleting a Report Group 6
Report Queries 7
Modifying an Existing Report Query 7
Creating a New Report Query 39
Deleting a Report Query 40
Copying and Pasting Queries 40
Scheduling Reports 41
Additional Functions 42
Email Settings 42

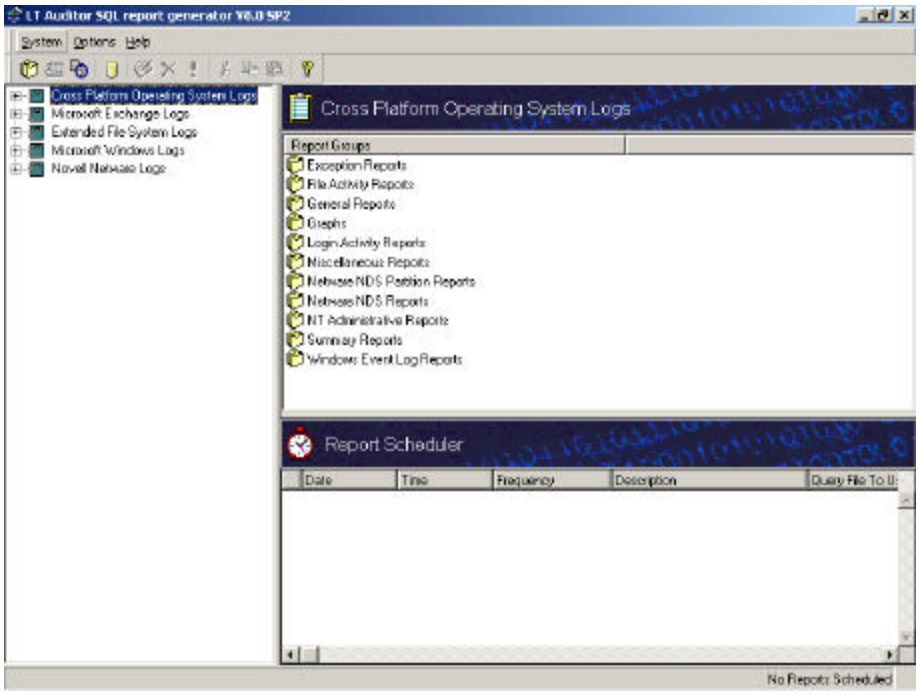
Appendix

Appendix A — Additional Features and Modifications

LT Auditor+ 8.0 SP2 SQL Report Generator

Chapter 1 — Overview

Report Generator



The Report Generator is an application used to run reports on server data collected by LT Auditor+ on the servers. Customizable reports query and export data to multiple formats.

Blue Lance offers several packages for LT Auditor+ 8.0 Service Pack (SP) 2. Depending on the license key purchased, you might see some or all of the packages listed below. These include:

- **Cross Platform Operating System Logs** — Create reports based on audited data from Microsoft Windows and Novell NetWare logs.
- **Microsoft Exchange Logs (Beta)** — Create reports based on audited data from Exchange logs
- **Extended File System Logs** — Create reports based on audited data from extended file system logs
- **Microsoft Windows Logs** — Create reports based on audited data from Windows logs
- **Novell NetWare Logs** — Create reports based on audited data from NetWare logs

Each package contains multiple query groups, such as:

- Exception reports
- File activity reports
- General reports
- Graphs
- Login activity reports
- Miscellaneous reports
- NetWare NDS partition reports
- NetWare NDS reports
- NT Administrative reports
- Summary reports
- Windows Event Log reports

A query groups consists of various report queries that allow you to generate a report. You can also create your own groups and custom report queries.

Each report can be viewed using the following formats:

- Crystal Reports
- Data Interchange Format (.dif)
- Web page (.html)
- Portable Document Format (.pdf)
- Report Definition format
- Record format
- Rich text format (.rtf)
- Comma separated descriptions
- Text format (.txt)
- Lotus 1-2-3 format
- Microsoft Word for Windows
- Microsoft Excel for Windows

LT Auditor+ 8.0 SP2 SQL Report Generator

Chapter 2 — Installing the Report Generator

Overview

The Report Generator uses the Crystal Report engine to generate reports, which provides features such as exporting to multiple data formats. For example, a user can export data to HTML format, allowing the reports to be viewed using an Internet browser.

Using a built-in scheduler, the Report Generator can run reports without user interaction. Scheduled reports reduce administrative overhead and lower ownership costs.

Requirements

The minimum requirements for installing the Report Generator include:

- Hardware
  - Intel Pentium processor 166 MHz or faster
  - 128 MB RAM
  - 100 MB available disk space (does not include requirements for the database)
- Software
  - One of the following Microsoft operating systems:
    - Windows NT with SP6 and Microsoft Internet Explorer 5
    - Windows 2000 with SP2
  - User rights to the registry located in the following directory: (HKEY_LOCAL_MACHINE\SOFTWARE\Blue Lance, Inc\LT Auditor+\)
  - Administrator rights to the report installation path

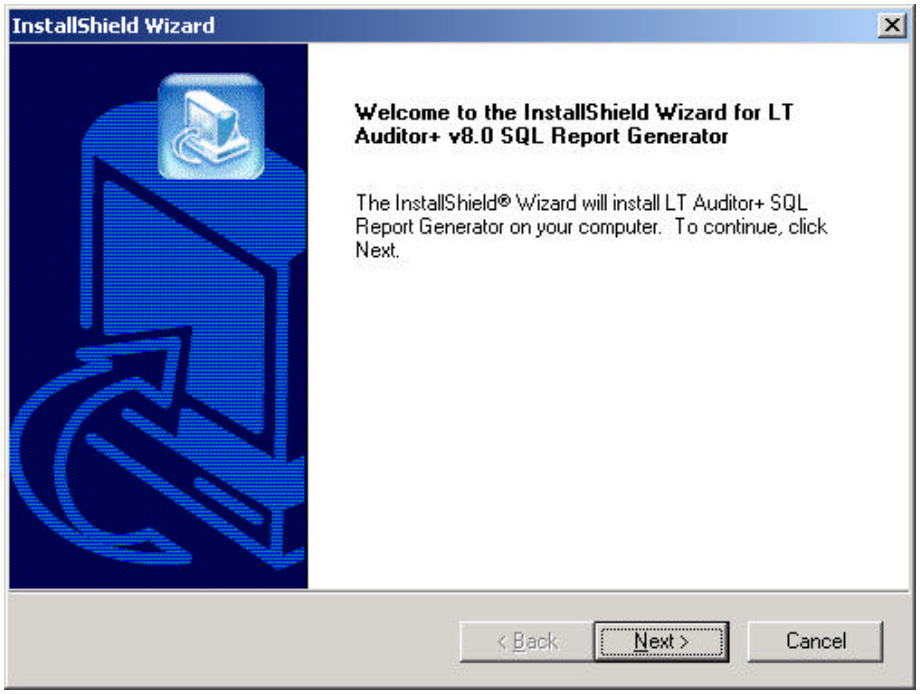
Installing the Report Generator

The Report Generator installs a set of report groups; each report group has its own specific queries. You can generate a report either by creating a report query or by using a built-in query, which can be applied to an LT Auditor+ data file.

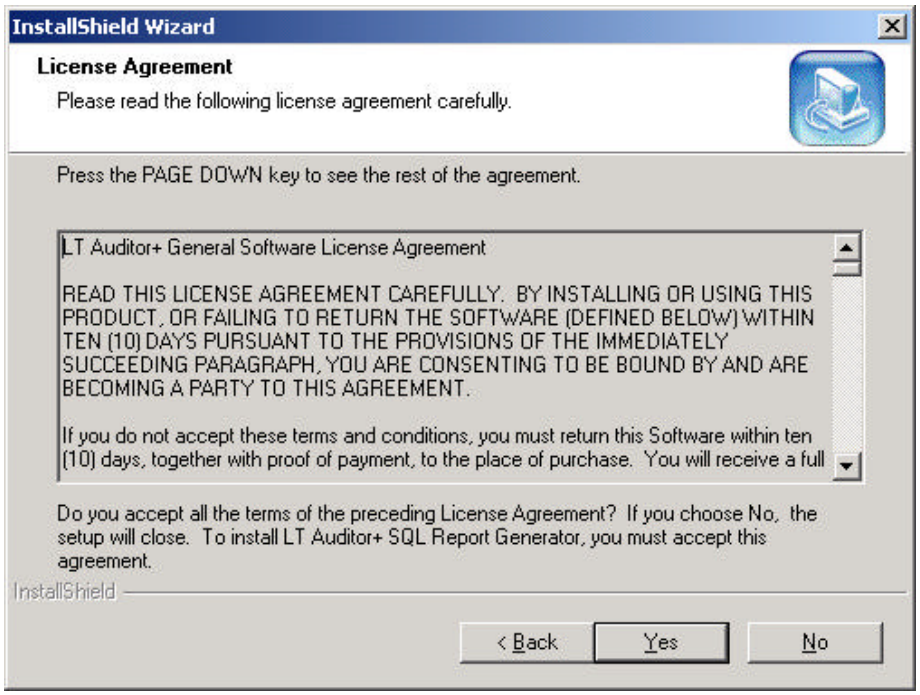
To install Report Generator, perform the following steps:

1. Insert the LT Auditor+ CD into the CD-ROM drive of the server or workstation.
2. If Autorun is enabled, select *Report Generator→ SQL Reports* when the following screen displays. If Autorun is not enabled, execute *Setup.exe* from the SQL Reports directory on the CD.

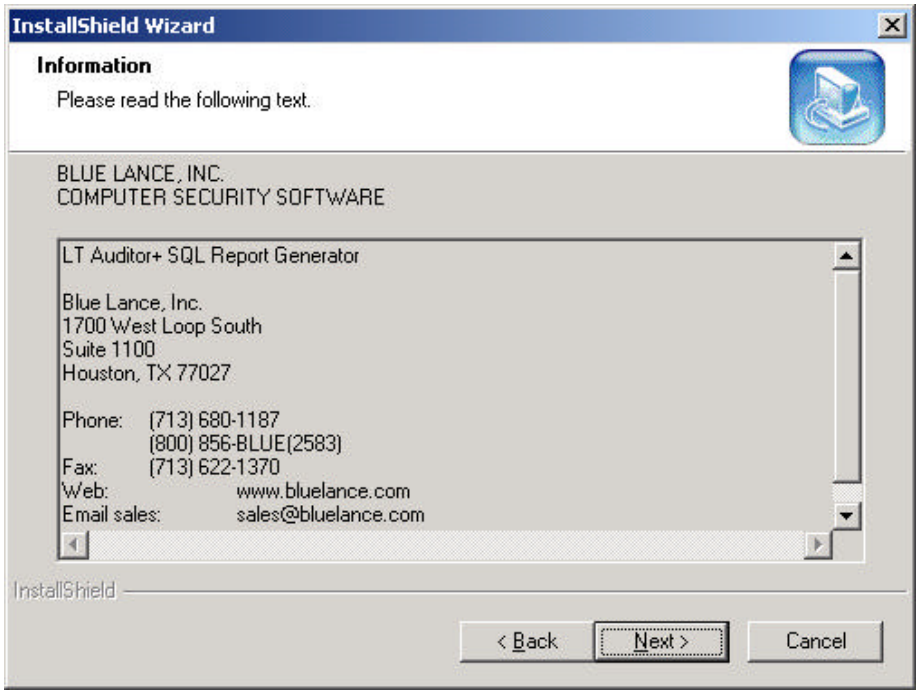
3. The InstallShield Wizard displays a welcome message. Click *Next* to display the License Agreement window.


InstallShield Wizard
Welcome to the InstallShield Wizard for LT Auditor+ v8.0 SQL Report Generator
The InstallShield® Wizard will install LT Auditor+ SQL Report Generator on your computer. To continue, click Next.
< Back
Next >
Cancel

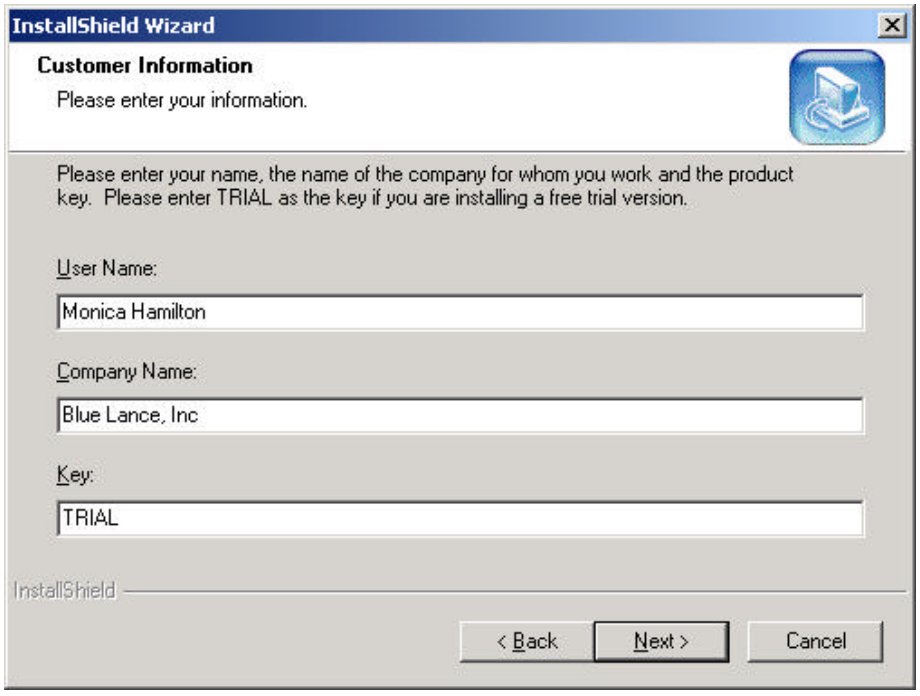
4. Press the *Page Down* key to read the entire agreement. Click *Yes* to accept the terms.


InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
LT Auditor+ General Software License Agreement
READ THIS LICENSE AGREEMENT CAREFULLY. BY INSTALLING OR USING THIS PRODUCT, OR FAILING TO RETURN THE SOFTWARE (DEFINED BELOW) WITHIN TEN (10) DAYS PURSUANT TO THE PROVISIONS OF THE IMMEDIATELY SUCCEEDING PARAGRAPH, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT.
If you do not accept these terms and conditions, you must return this Software within ten (10) days, together with proof of payment, to the place of purchase. You will receive a full
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install LT Auditor+ SQL Report Generator, you must accept this agreement.
InstallShield
< Back
Yes
No

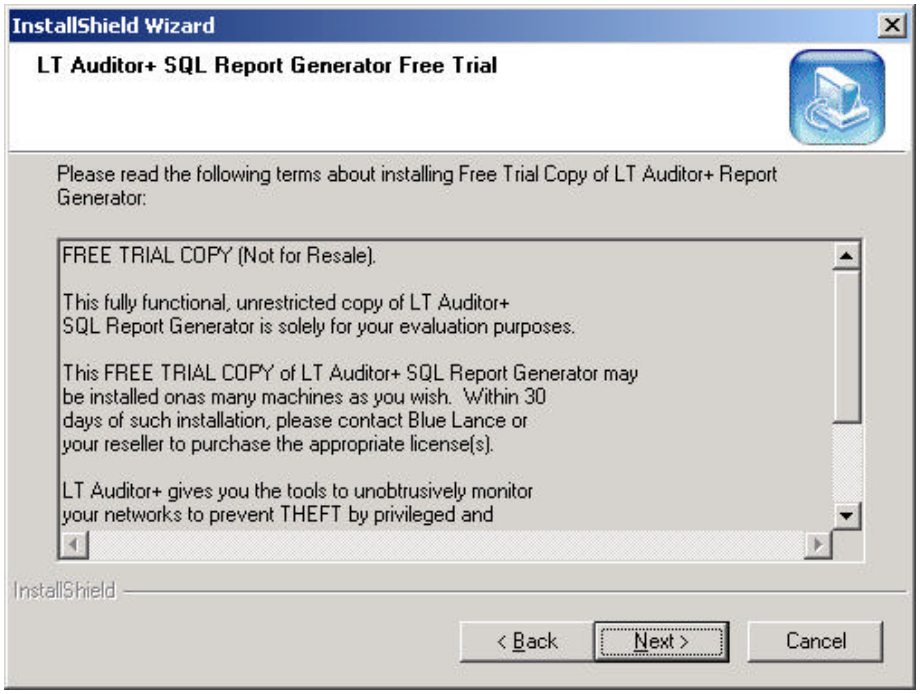
5. The Information window displays the Blue Lance contact information. Review the information, then click *Next* to display the Customer Information window.



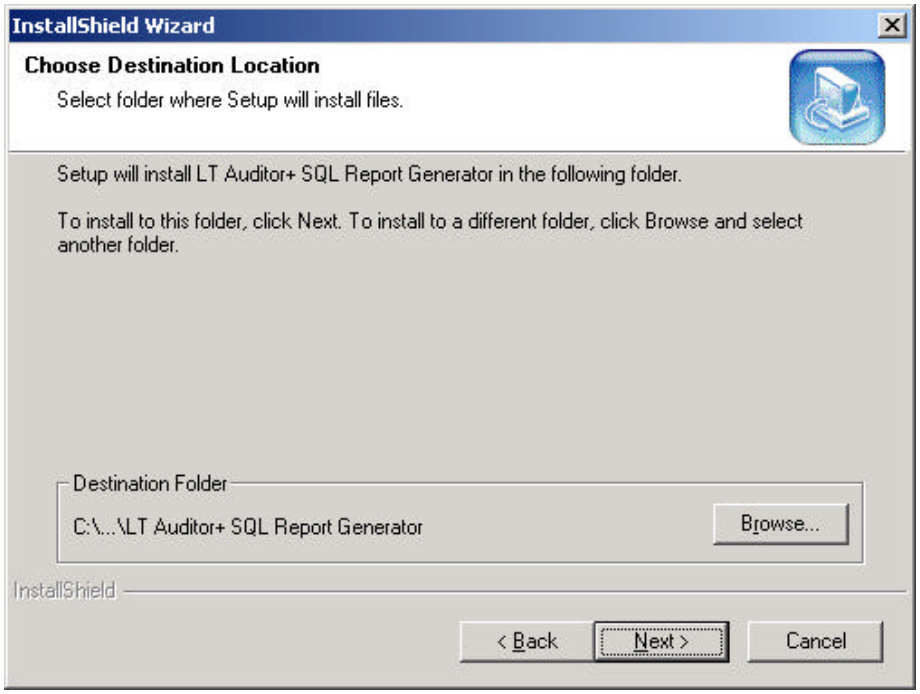
6. Enter your user name, company name, and key. If you are installing a trial version of the Report Generator, enter *Trial* in the Key field. Click *Next* to display the Choose Destination Location window.


InstallShield Wizard
Customer Information
Please enter your information.
Please enter your name, the name of the company for whom you work and the product key. Please enter TRIAL as the key if you are installing a free trial version.
User Name:
Monica Hamilton
Company Name:
Blue Lance, Inc
Key:
TRIAL
InstallShield
< Back
Next >
Cancel

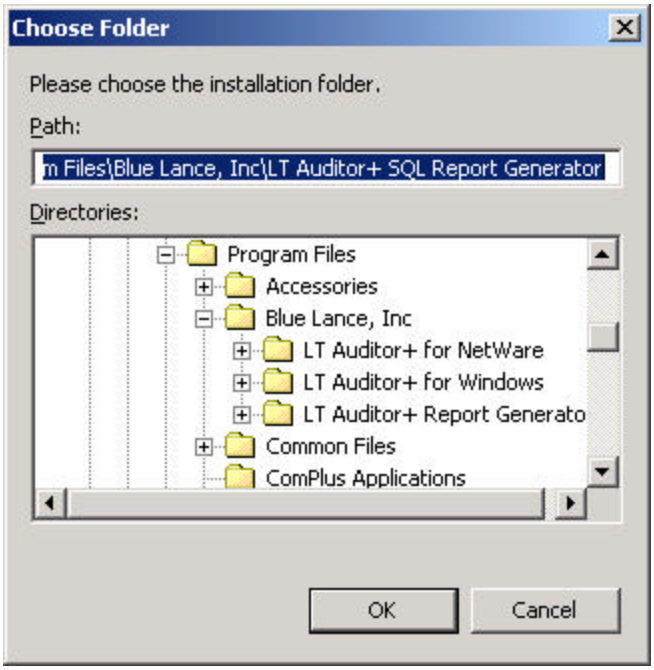
7. If you entered Trial in the key field, the LT Auditor+ SQL Report Generator Free Trial window will display. Click *Next* to accept the terms and conditions of this trial installation.


InstallShield Wizard
LT Auditor+ SQL Report Generator Free Trial
Please read the following terms about installing Free Trial Copy of LT Auditor+ Report Generator:
FREE TRIAL COPY (Not for Resale).
This fully functional, unrestricted copy of LT Auditor+ SQL Report Generator is solely for your evaluation purposes.
This FREE TRIAL COPY of LT Auditor+ SQL Report Generator may be installed onas many machines as you wish. Within 30 days of such installation, please contact Blue Lance or your reseller to purchase the appropriate license(s).
LT Auditor+ gives you the tools to unobtrusively monitor your networks to prevent THEFT by privileged and
InstallShield
< Back
Next >
Cancel

8. From the Choose Destination Location window, click *Next* to accept the default location, or click *Browse* to change the location for the Report Generator files. The Choose Folder window displays.

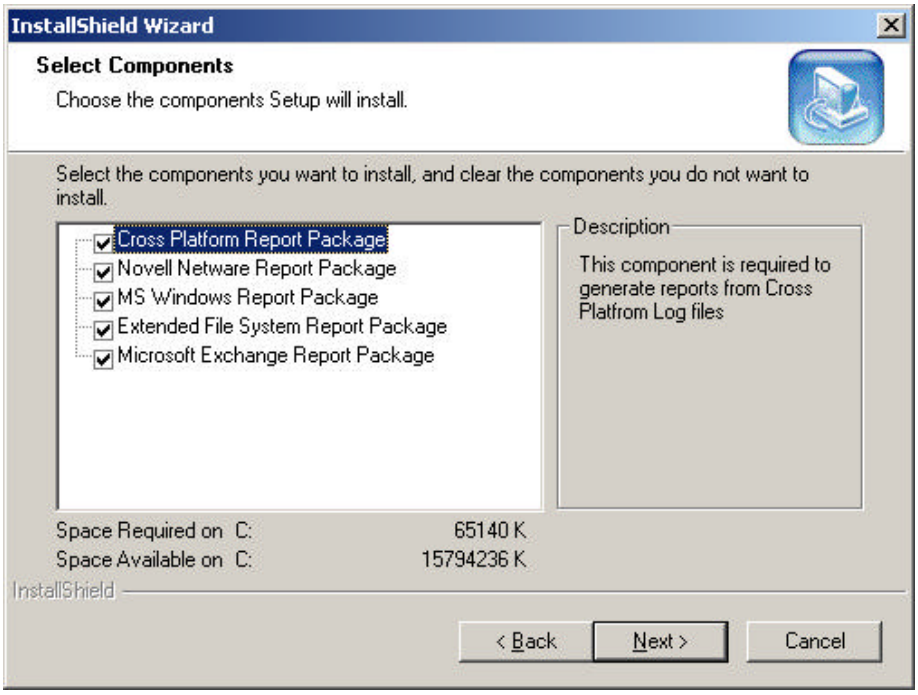

InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install LT Auditor+ SQL Report Generator in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\LT Auditor+ SQL Report Generator
Browse...
InstallShield
< Back
Next >
Cancel

9. From the Choose Folder window, select the location where the Report Generator files will be stored and click *OK* → *Next*.



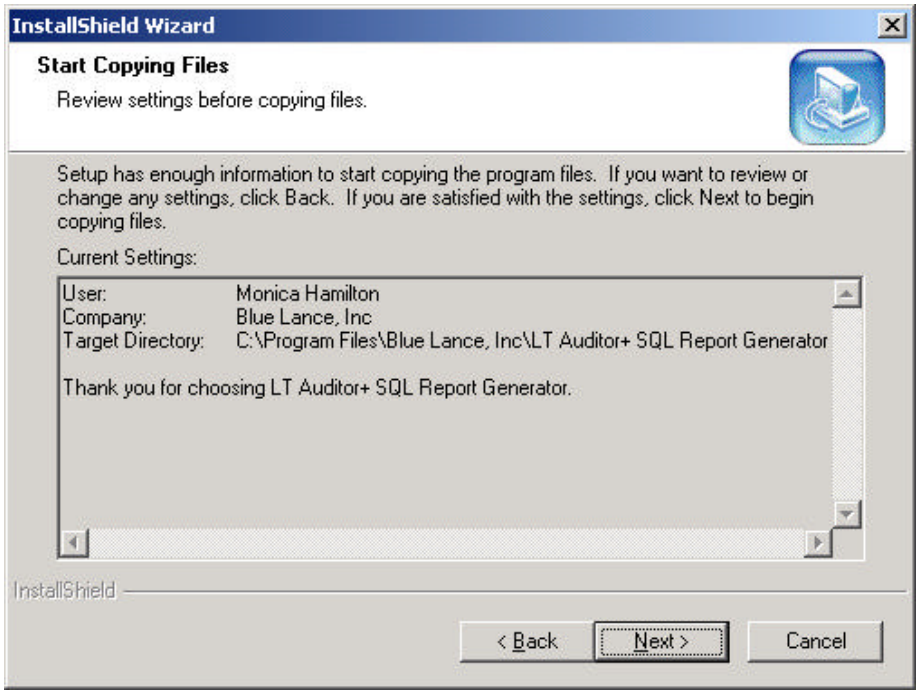
10. When the Select Components window displays, the following options are selected by default:

    - **Cross Platform Report Package** — Generates reports from Cross Platform log files
    - **Novell NetWare Report Package** — Generates reports from NetWare log files
    - **Microsoft Windows Report Package** — Generates reports from Microsoft Windows log files
    - **Extended File System Report Package** — Generates reports from Extended File System log files
    - **Microsoft Exchange Report Package** — Generates reports from Microsoft Exchange log files

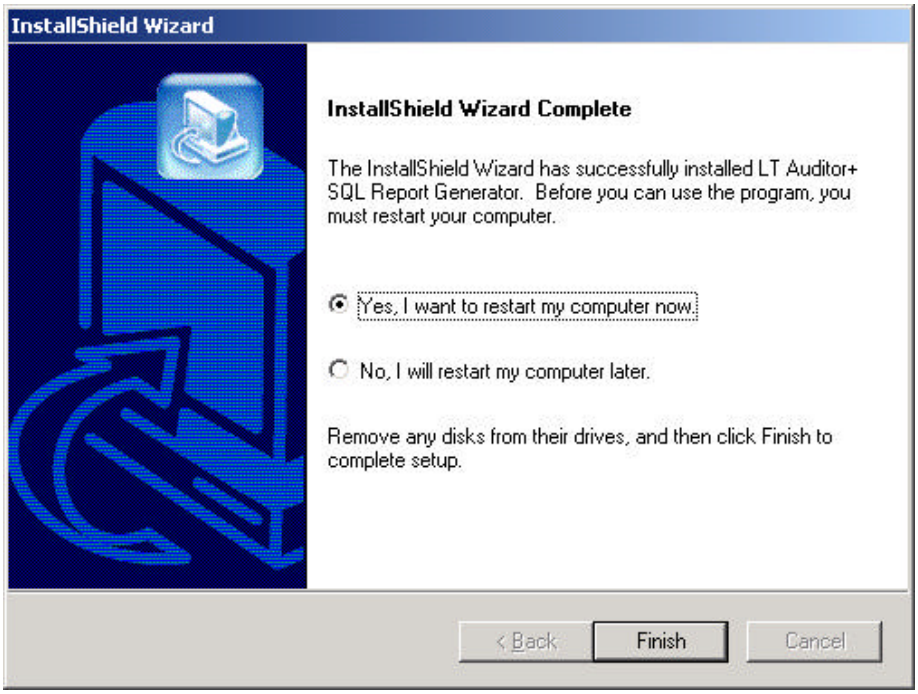

InstallShield Wizard
Select Components
Choose the components Setup will install.
Select the components you want to install, and clear the components you do not want to install.
Cross Platform Report Package
Novell Netware Report Package
MS Windows Report Package
Extended File System Report Package
Microsoft Exchange Report Package
Description
This component is required to generate reports from Cross Platfrom Log files
Space Required on C: 65140 K
Space Available on C: 15794236 K
InstallShield
< Back
Next >
Cancel

To deselect a package, click the check box located to the left of the package you do not want to install. Click *Next*.

11. The Start Copying Files window displays the setup information for your Report Generator files. Click *Next*.


InstallShield Wizard
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
User: Monica Hamilton
Company: Blue Lance, Inc
Target Directory: C:\Program Files\Blue Lance, Inc\LT Auditor+ SQL Report Generator
Thank you for choosing LT Auditor+ SQL Report Generator.
InstallShield
< Back
Next >
Cancel

12. The files are copied to the specified location and the InstallShield Wizard Complete window displays. By default, the *Yes, I want to restart my computer now* option is selected. Click *Finish* to complete the installation process.


InstallShield Wizard
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed LT Auditor+ SQL Report Generator. Before you can use the program, you must restart your computer.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
< Back
Finish
Cancel

LT Auditor+ 8.0 SP2 SQL Report Generator
Chapter 3 — Constructing a Database

Overview

This chapter contains instructions on constructing a database using:

- Microsoft SQL Server 2000 and SQL Server 7.0
- Oracle8*i* database products

Space Considerations

To optimize the performance of LT Auditor+, there must be sufficient storage space for the LT Auditor+ database. The storage space required varies greatly depending on the:

- Number of servers on which LT Auditor+ is installed.
- Number of users per server.
- Policies set for auditing.
- Length of time the data will be stored.

  Example

  If a company collects the equivalent of one million records, 125 MB of space or more is required for the LT Auditor+ database.

  As the number of logs collected increases, the size of the database will also increase. You can determine the hard drive space required for the LT Auditor+ database according to the amount of audit data you collect.

Constructing a SQL Database

LT Auditor+ for Windows is designed to work with SQL Server 2000/SQL Server 7.0 databases. Before constructing a database, you must install SQL Server using the following default options:

- Code page 1252
- Dictionary order, case-insensitive

Note
Code pages and sort orders other than the default are not currently supported and can cause unexpected results.

Any computer with SQL Server 2000 or SQL Server 7.0 properly installed should be satisfactory for the creation of the LT Auditor+ database. For requirements to install SQL Server, refer to the Microsoft website at: **http://www.microsoft.com**

Using SQL Server 2000 and SQL Server 7.0, you can create two types of databases:

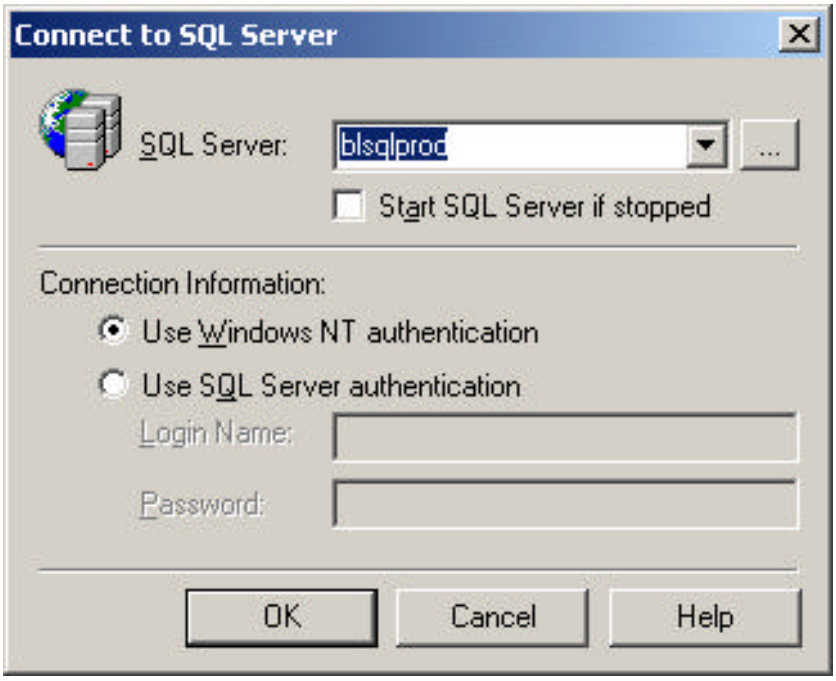
- Basic
- Custom

Note
The following sections contain screen captures from SQL Server 2000.

Creating a Basic Database

To create a basic database, perform the following steps:

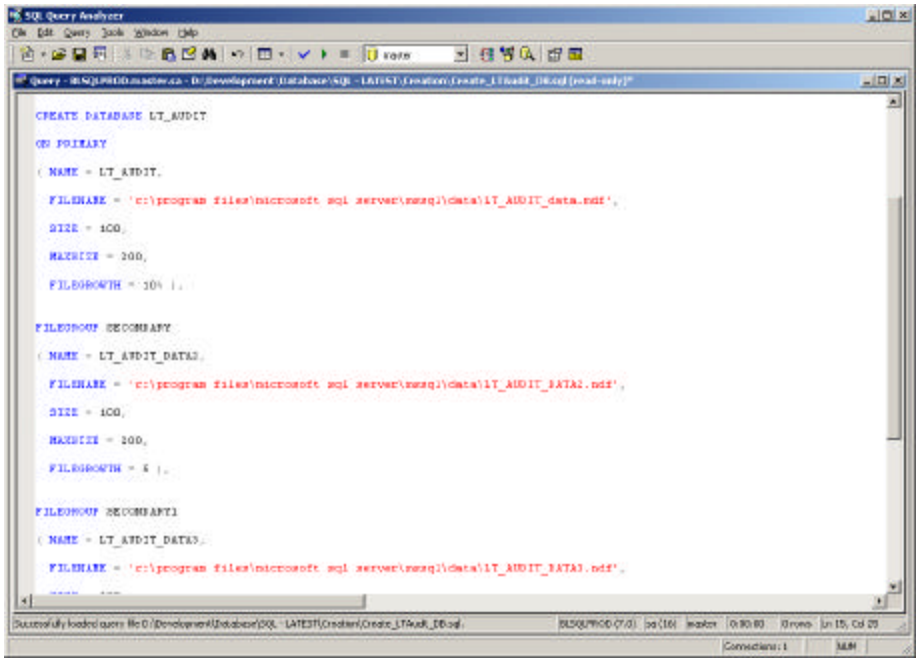
1. On your computer desktop, click *Start* → *Programs* → *Microsoft SQL Server* → *Query Analyzer* to display the Connect to SQL Server window.



2. In the SQL Server field, enter the name of your SQL Server.

Note
This procedure must be performed on a computer with SQL Server client access tools installed.

3. Under Connection Information, select *Use Windows NT authentication* to accept the login name and password assigned by the operating system. Select *Use SQL Server authentication* to enter a SQL Server login name and password. Click *OK* to continue. The SQL Query Analyzer window will display.

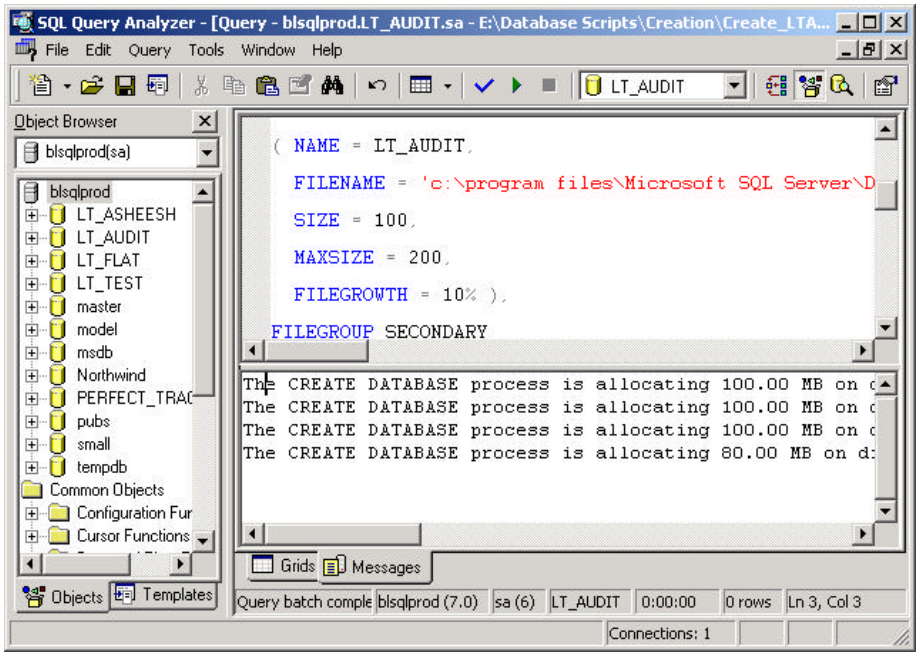


4. Insert the LT Auditor+ CD into the CD-ROM drive of your SQL Server computer.
5. From the Standard toolbar, select the *Load SQL Script* button .
6. Open the Database Creation Script.sql file located on the LT Auditor+ CD in the Database Scripts\Microsoft SQL Server directory. Click *Open*.

7. The default path for the database files is C:\program files\Microsoft SQL Server\mssql\data\. Refer to the Space Considerations section in this chapter before making any modifications to the path and the size of the database. Verify on the Messages tab that the database has been created.

Note

The default path, C:\program files\Microsoft SQL Server\mssql\data\, is specific to SQL Server 2000. Modify this path based on your business and technical requirements.



8. After the database is created, if you are using SQL 2000, you must change the Recovery model to *Simple* from the Options tab. If you are using SQL Server 7.0, from the Options tab under Settings, check the *Truncate log on checkpoint* check box.

!

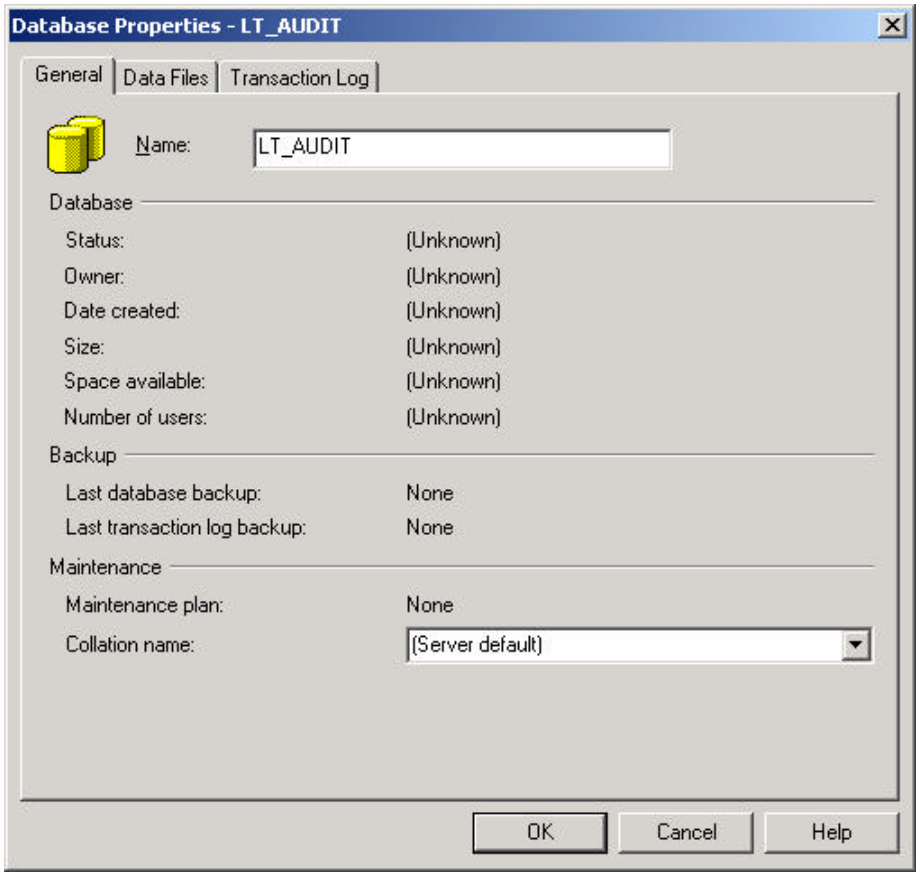
Important

You must click the *Execute Query* button , located on the Standard toolbar, to save changes.

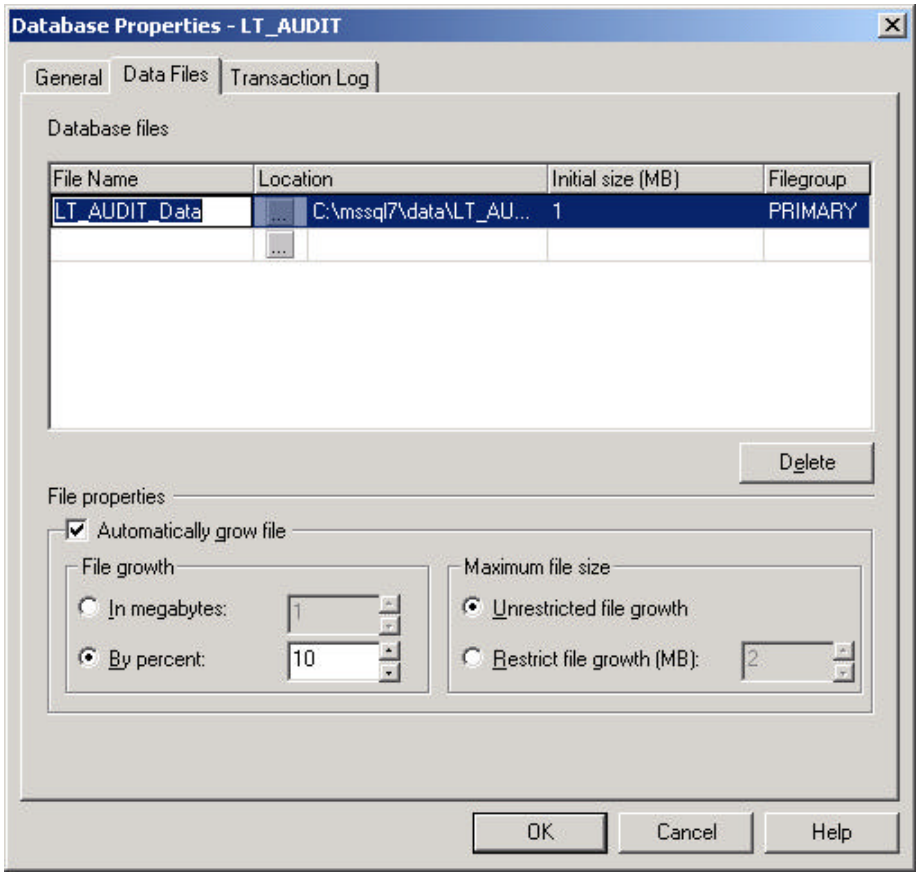
Creating a Custom Database

To create a custom database, perform the following steps:

1. On your computer desktop, click Start → Programs → Microsoft SQL Server → Enterprise Manager.
2. Select the server on which the new database will be created.
3. From the Action menu, select *New Database*.
4. In the Database Properties window, select the *General* tab. In the name field, enter *LT_AUDIT*.



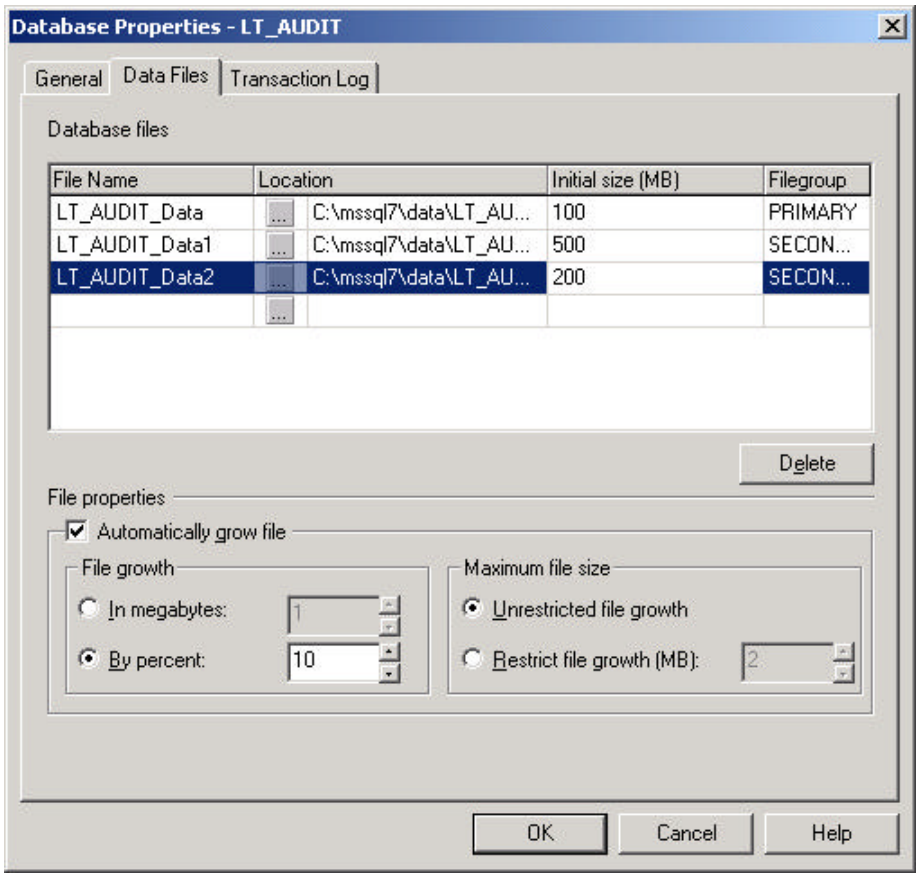
5. Select the *Data Files* tab. Under File Name, enter *LT_AUDIT_Data.*



6. Keep the default location or specify a different location where you want the database to reside. If you want to change the location of the database, click the *Location* button. From the Locate Database File window, select the location of your database and click *OK*.
7. Under Filegroup, enter *Primary*. The scripts for table creation are designed to work with three file groups:
   1. Primary
   2. Secondary
   3. Secondary1

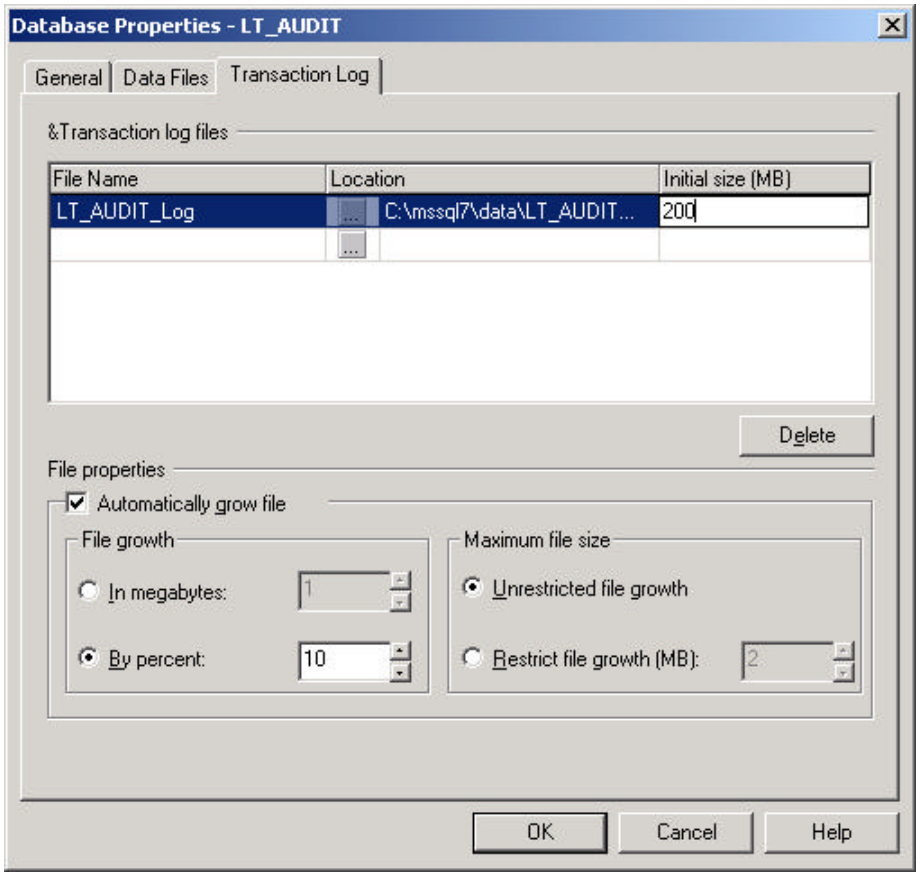
   Spreading data files across multiple groups yields better performance from the database.

8. In the second row, under File Name, enter *LT_AUDIT_Data1*. Keep the default location or specify a different location where you want the database to reside. Under Filegroup, enter *Secondary*.
9. In the third row, under File Name, enter *LT_AUDIT_Data2*. Keep the default location or specify a different location where you want the database to reside. Under Filegroup, enter *Secondary1*.



10. Under File properties, the check box *Automatically grow file* is selected by default. This feature allows the currently selected file to grow automatically as more data space is needed. To specify the file growth, select *In megabytes* or *By percent* and enter the value.
11. Under Maximum file size, you can limit the file size. Select from these options:
    4. Unrestricted File Growth — Allows the file to grow as large as necessary.
    5. Restrict file growth (MB) — Allows you to specify the maximum size in megabytes to which the file should be allowed to grow.

12. Click the *Transaction Log* tab. In the Initial size field, enter a number that represents 25-30% of the space allotted for your database. Click *OK* to save changes.



13. After the database is created, if you are using SQL 2000, you must change the Recovery model to *Simple* from the Options tab. If you are using SQL Server 7.0, from the Options tab under Settings, check the *Truncate log on checkpoint* check box.

Creating Tables, Views, Stored Procedures, and Audit Triggers

After the database has been created, you must create the structure within the database for LT Auditor+ to run properly. This structure comprises four database components:

- Tables
- Views
- Stored procedures
- Audit triggers

To create the structure within the database:

1. Click *Start ® Programs ® Microsoft SQL Server ® Query Analyzer* to display the SQL Server Query Analyzer window. The Connect to SQL Server window displays. Connect to the SQL Server where the database was created. Click *OK*.
2. From the Current Database drop-down menu, select the database created for LT Auditor+.
3. At the root of the LT Auditor+ CD, click *Database Scripts → Microsoft SQL Server → Objects Creation Script*.
4. Click *Execute Query* to create the tables, indexes, and constraints.

Creating Tables, Views, and Stored Procedures for Exchange Logs

If you are auditing Exchange logs, you must create objects within that database. To create the objects within the database:

1. Click *Start ® Programs ® Microsoft SQL Server ® Query Analyzer* to display the SQL Server Query Analyzer window. The Connect to SQL Server window displays. Connect to the SQL Server where the database was created. Click *OK*.
2. From the Current Database drop-down menu, select the database created for LT Auditor+.
3. At the root of the LT Auditor+ CD, click *Database Scripts → Microsoft SQL Server → Objects Creation Script for Exchange*.
4. Click *Execute Query* to create the tables, indexes, and constraints.

Creating Tables, Views, and Stored Procedures for Extended File System Logs

If you are auditing Extended File System logs, you must create objects within that database. To create the objects within the database:

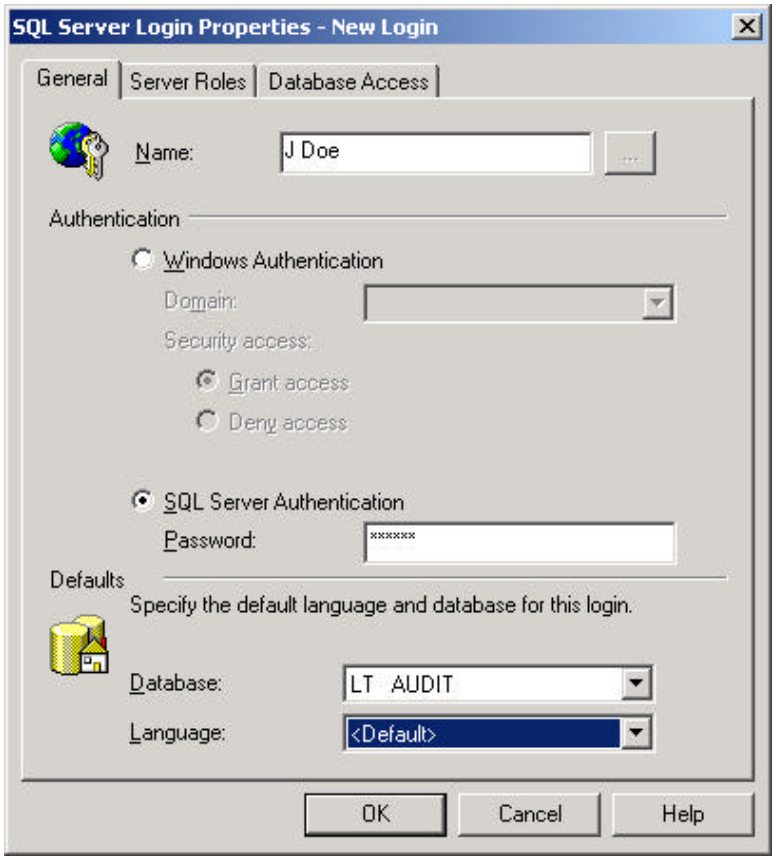
1. Click *Start ® Programs ® Microsoft SQL Server ® Query Analyzer* to display the SQL Server Query Analyzer window. The Connect to SQL Server window displays. Connect to the SQL Server where the database was created. Click *OK*.
2. From the Current Database drop-down menu, select the database created for LT Auditor+.
3. At the root of the LT Auditor+ CD, click *Database Scripts → Microsoft SQL Server → Objects Creation Script for File System*.
4. Click *Execute Query* to create the tables, indexes, and constraints.

Assigning Permissions to the Database

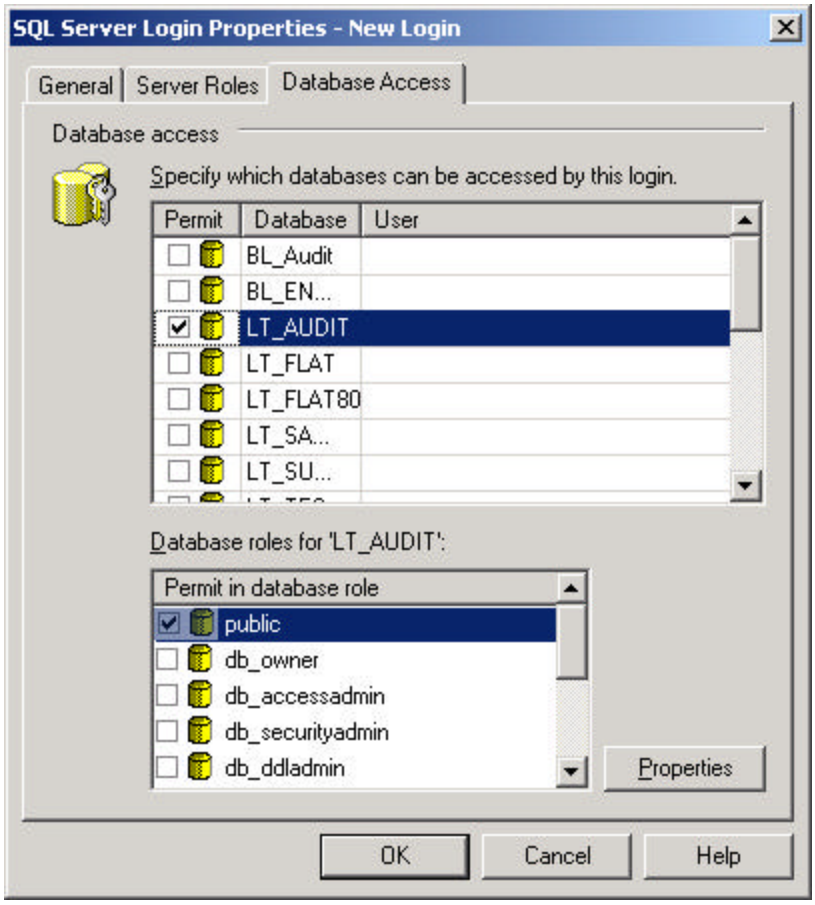
To maintain the security of LT Auditor+ database, it is necessary to assign the appropriate permission to the person consolidating the data and running the reports. You can assign the permissions manually or you can use the Database Login Wizard to guide you through the process. Assigning permissions manually allows users to configure server roles and database access for a specified user.

To assign permissions, perform the following steps:

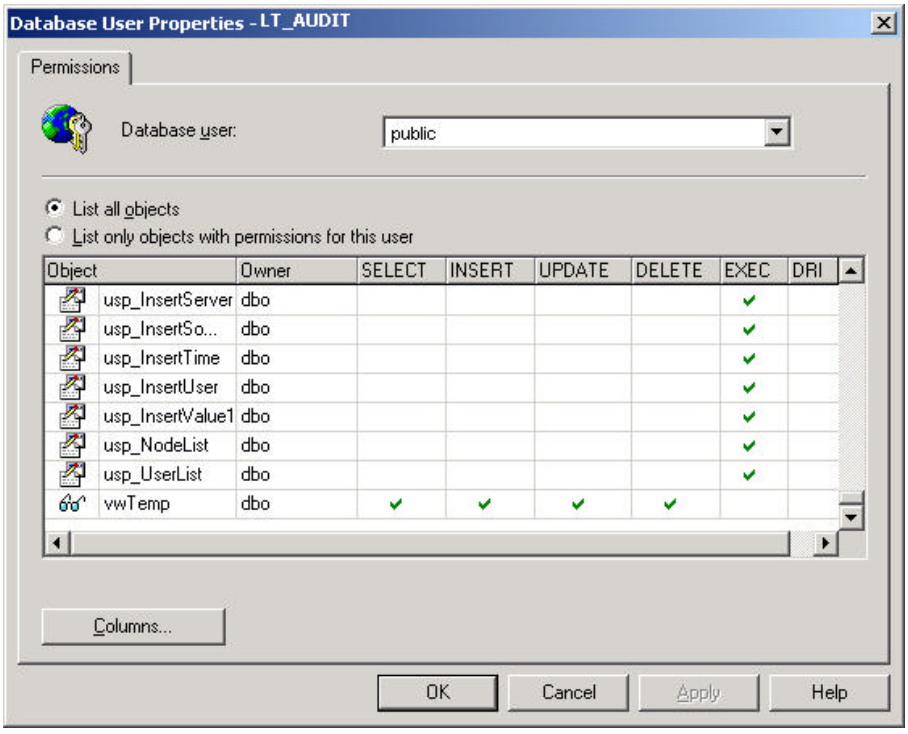
1. Click Start → Programs → Microsoft SQL Server → Enterprise Manager.
2. In the Enterprise Manager window, click *Security*. Under Security, right-click *Login*. On the drop-down menu, select *New Login*. The SQL Server Login Properties – New Login window displays.
3. Select the *General* tab. In the Name field, enter the new user name. Under Authentication, select the SQL Server Authentication button. Enter your SQL Server password.



4. Select the *Database Access* tab. From this screen, you can specify the permissions of the selected user. Select the database to which you want to grant the user rights.



5. Click *Properties* → *Permissions* to display the Database User Properties – LT_AUDIT window.



Note

The eyeglass icon in the Object column identifies the views; the file icon in the Object column identifies the stored procedures.

6. To ensure that the user has minimum rights to the SQL Report Generator, perform the following steps in the SELECT column:
   - On all views that are dbo owned, put a check mark in the SELECT column.
   - On all stored procedures that are dbo owned, put a check mark in the EXEC column.

Important

Only the SELECT and EXEC rights should be modified.

7. Click *OK* to exit the Database User Properties – Properties LT_AUDIT window.

Creating a Maintenance Plan for SQL Server

Blue Lance recommends that you follow the recommended practices from Microsoft for maintenance of the LT Auditor+ database. Blue Lance recommends that you:

- Back up your database daily to a tape or a hard drive. A backup wizard is provided in the Enterprise Manager window to guide you through this process. To access the Enterprise Manager window, select *Start* → *Programs* → *Microsoft SQL Server* → *Enterprise Manager.*
- Restore the database periodically from the backup to a hard drive or a test database to ensure the validity of the backup.
- Create a maintenance plan with the Enterprise Manager and the Maintenance Wizard.

Because the insertion process is longer when the data and index pages are full, reorganizing the pages for maximum efficiency improves the database performance.

A good maintenance plan will have:

- A database integrity check and index rebuilding.
  - The Integrity Check window allows you to include, exclude and modify indexes.
  - The Index Rebuilding window enhances performance by deleting an index and creating a new index.
- Consistency checks of the data and data pages to ensure there is no data corruption.
- File compression by removing empty database pages.

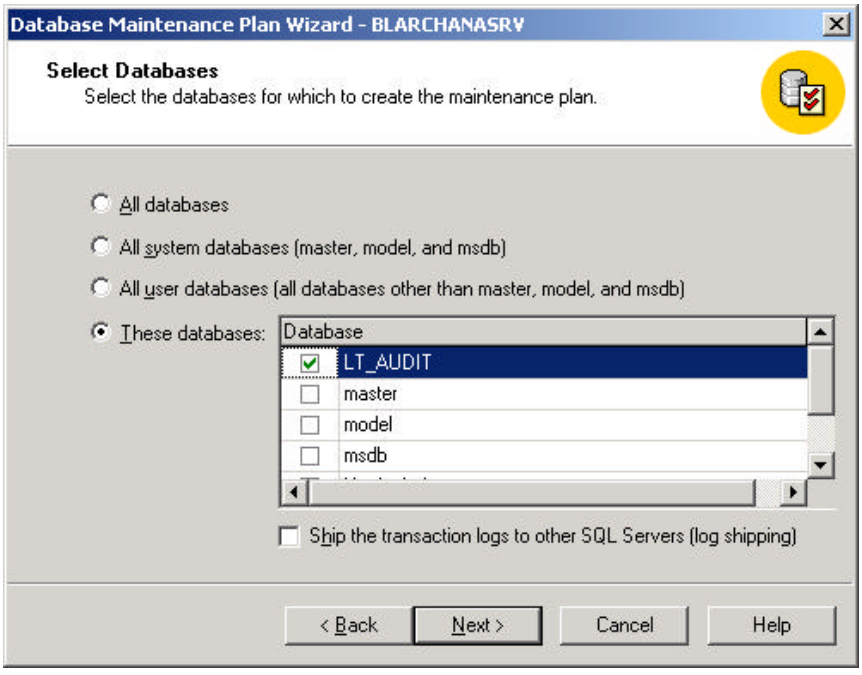
The following steps provide a basic approach to creating a database maintenance plan. For detailed instructions, consult SQL Server help online at: **http://www.microsoft.com**

To create a maintenance plan using SQL Server, perform the following steps:

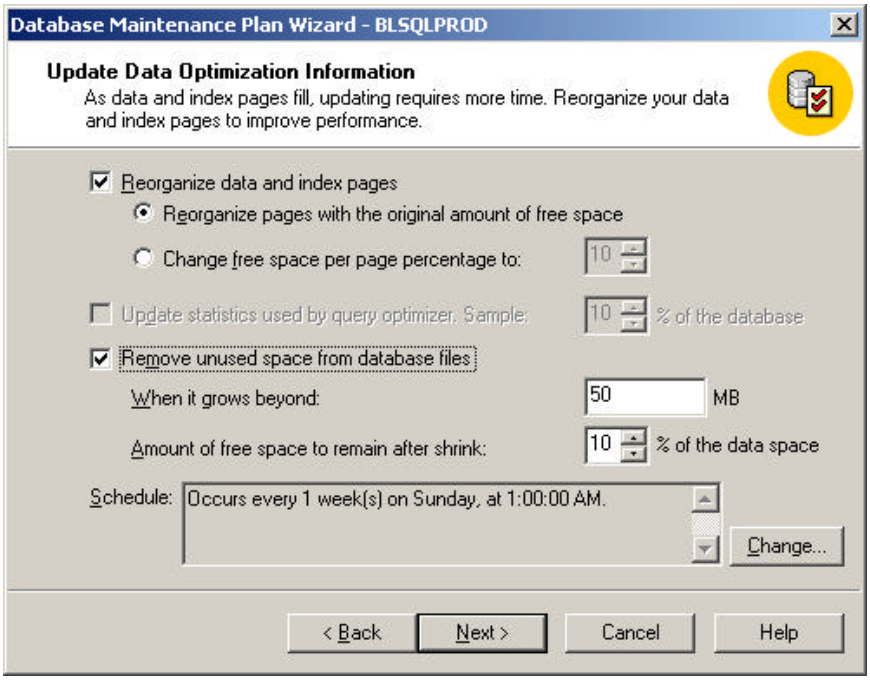
1. From the SQL Server Enterprise Manager tree under Management, right-click *Database Maintenance Plans* and select *New Maintenance Plan*. The Database Maintenance Plan Wizard window displays. Click *Next* to continue.

Database Maintenance Plan Wizard - BLARCHANASRV
Welcome to the Database Maintenance Plan Wizard
This wizard helps you create a maintenance plan that the SQL Server Agent can run on a regular basis. With this wizard you can:
Run database integrity checks.
Update database statistics.
Perform database backups.
Ship transaction logs to another server (Enterprise Edition).
< Back
Next >
Cancel
Help

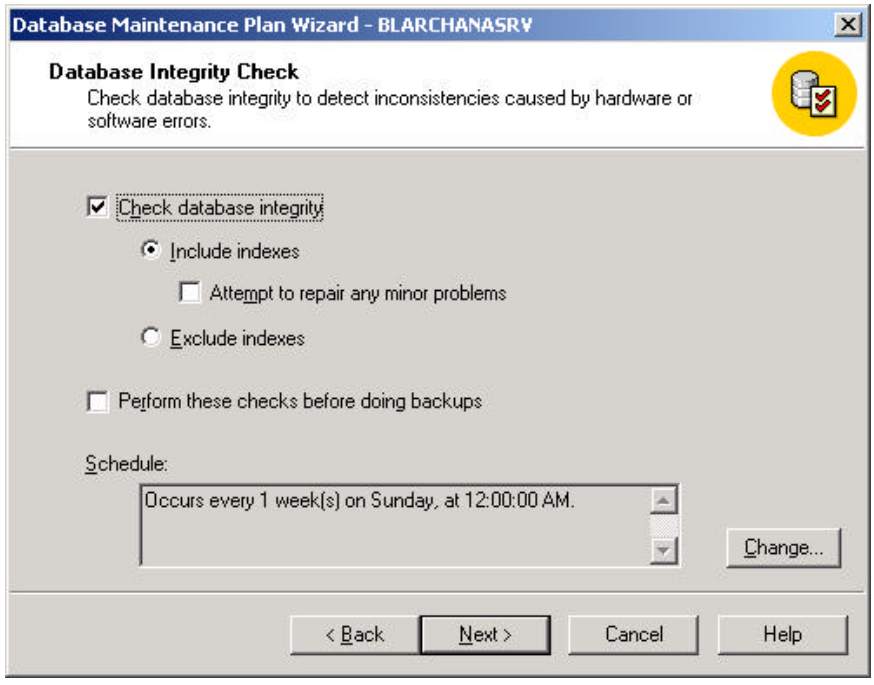
2. The Select Databases window displays. This window allows you to select single or multiple databases to manage. Click *These databases* and select the database you wish to manage. Click *Next* to continue.



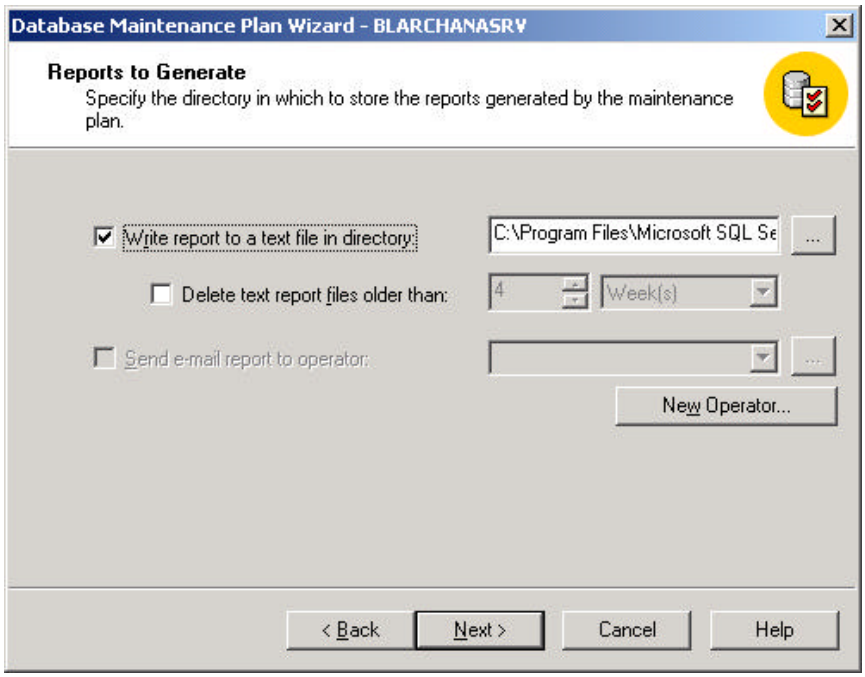
3. The Update Data Optimization Information window displays. Select *Reorganize data and index pages*, *Reorganize pages with the original amount of free space* and *Remove unused space from the database files*. Click *Next* to continue.


Database Maintenance Plan Wizard - BLSQLPROD
Update Data Optimization Information
As data and index pages fill, updating requires more time. Reorganize your data and index pages to improve performance.
Reorganize data and index pages
Reorganize pages with the original amount of free space
Change free space per page percentage to:
10
Update statistics used by query optimizer. Sample:
10
% of the database
Remove unused space from database files
When it grows beyond:
50
MB
Amount of free space to remain after shrink:
10
% of the data space
Schedule:
Occurs every 1 week(s) on Sunday, at 1:00:00 AM.
Change...
< Back
Next >
Cancel
Help

4. The Database Integrity Check window displays. Select *Check database integrity.* Click *Change* to display the Edit Recurring Job Schedule Modify window schedule the integrity check and click *OK*. Click *Next* to continue.


Database Maintenance Plan Wizard - BLARCHANASRV
Database Integrity Check
Check database integrity to detect inconsistencies caused by hardware or software errors.
Check database integrity
Include indexes
Attempt to repair any minor problems
Exclude indexes
Perform these checks before doing backups
Schedule:
Occurs every 1 week(s) on Sunday, at 12:00:00 AM.
Change...
< Back
Next >
Cancel
Help

5. Backups can be scheduled through the Maintenance Plan Wizard or they can be set up as a separate job. Click *Next* → *Next* to continue to identify the directory to store the reports generated.
6. When the Reports to Generate window displays, select *Write report to a text file in directory*. Click *Next* → *Next* → *Finish* to complete the Database Maintenance Plan Wizard.


Database Maintenance Plan Wizard - BLARCHANASRV
Reports to Generate
Specify the directory in which to store the reports generated by the maintenance plan.
Write report to a text file in directory:
C:\Program Files\Microsoft SQL Se
Delete text report files older than:
4
Week(s)
Send e-mail report to operator:
New Operator...
< Back
Next >
Cancel
Help

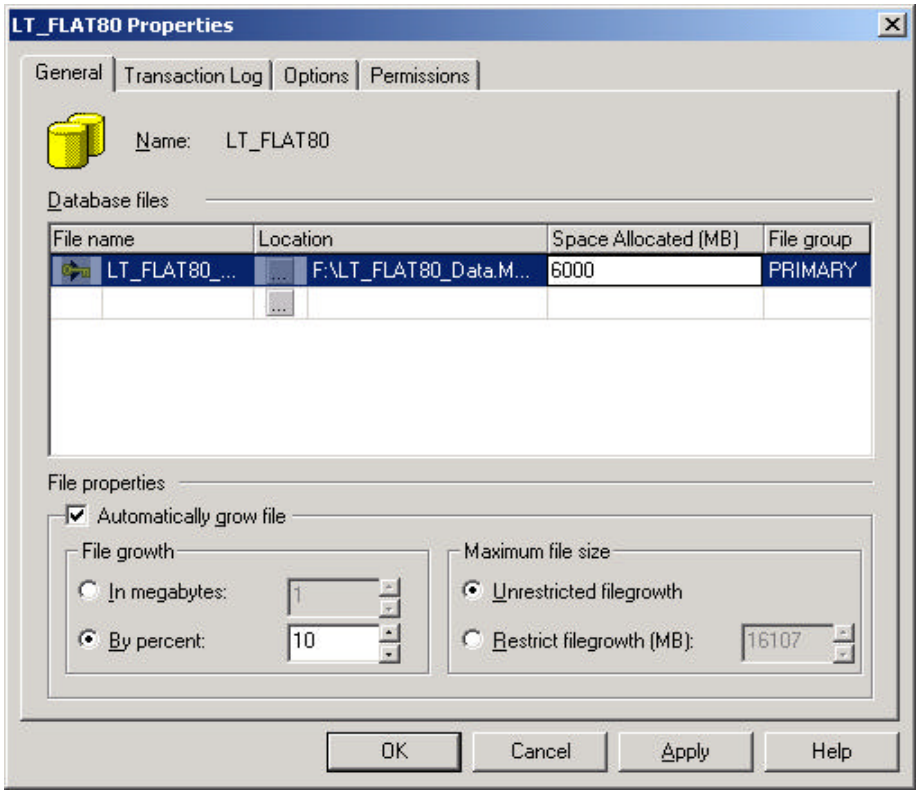
Archiving the Database and Deleting Data

To improve the performance of the current database, data needs to be archived to an Archive database and deleted from the current database. Perform the following steps to create a Flat database, which includes one file group, one table, and requires more disk space than the current database.

Creating a Flat Database

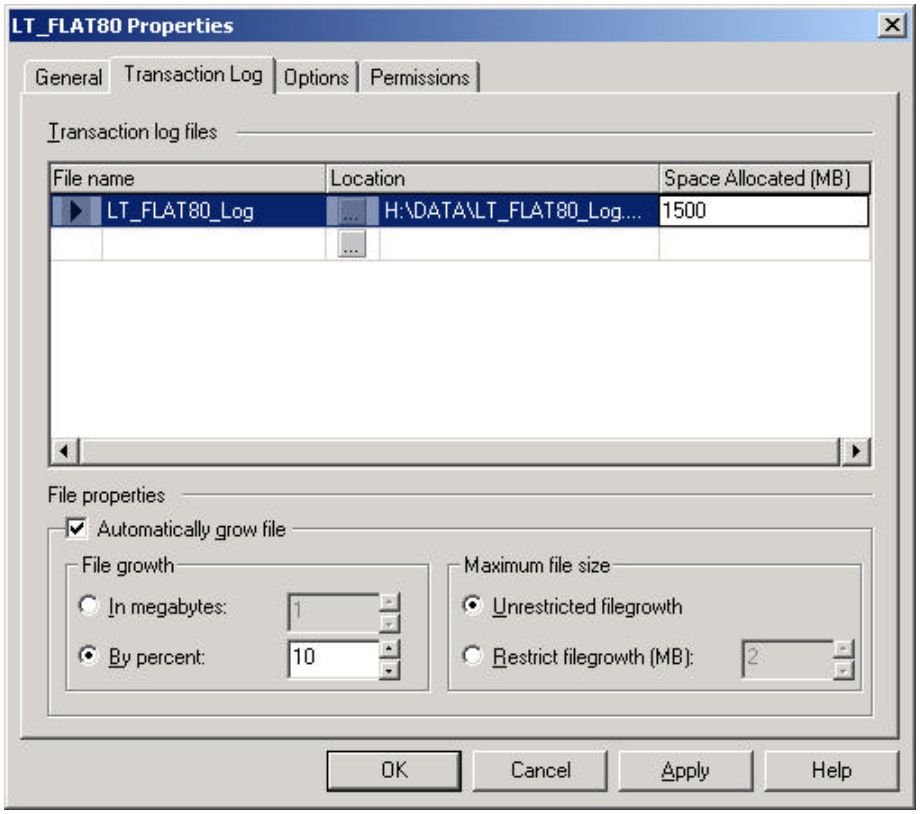
Display the Enterprise Manager and perform the following steps:

1. Create a database containing only the Primary file group.



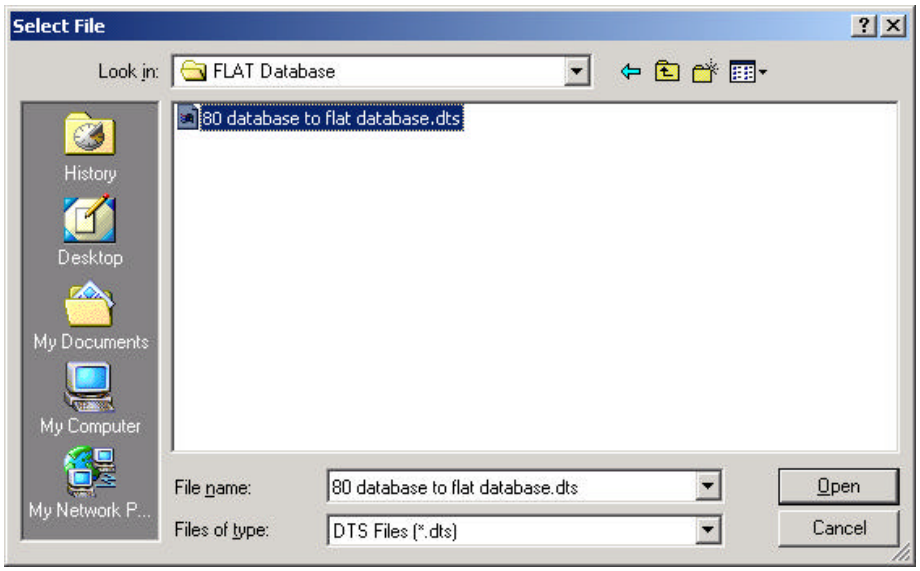
2. Allocate the space based on the database requirements.
3. Verify the number of records that will be inserted daily and the number of days or months the data will be stored. Calculate the size of the database based on the number of days or months that the data will be stored.

4. Create log files that are 25 to 30 percent of the entire database.

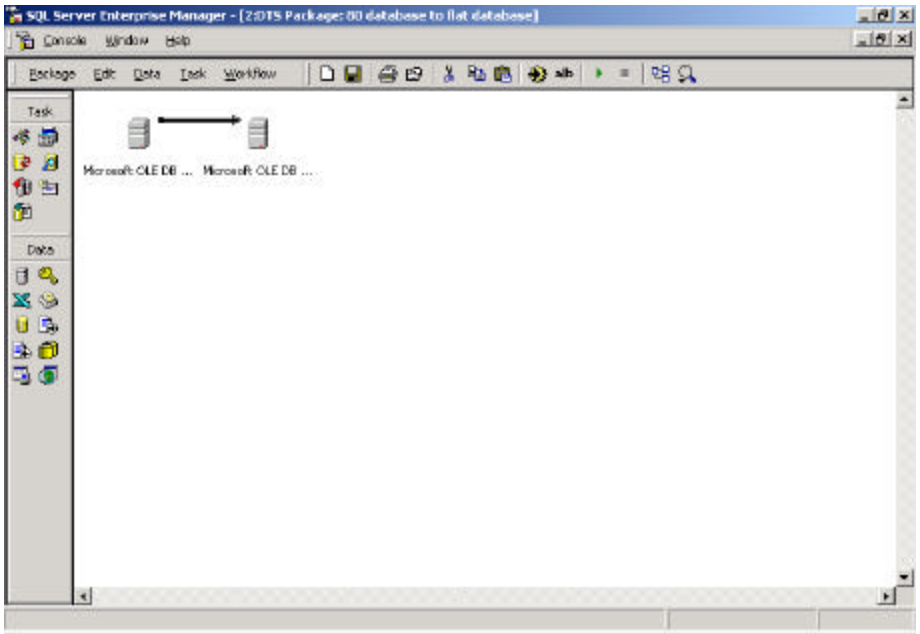


5. After the database is created, if you are using SQL 2000, from the Options tab change the Recovery model to *Simple*. If you are using SQL Server 7.0, from the Options tab under Settings, check the *Truncate log on checkpoint* check box.
6. After creating the database, run the scripts in Query Analyzer to create the table, views, and one deletion stored procedure.
   a. Click *Start ® Programs ® Microsoft SQL Server ® Query Analyzer* to display the SQL Server Query Analyzer window. The Connect to SQL Server window displays. Connect to the SQL Server where the database was created. Click *OK*.
   b. From the Current Database drop-down menu, select the database created for LT Auditor+.
   c. At the root of the LT Auditor+ CD, click *Database Scripts → Microsoft SQL Server → Create FlatDatabaseObjects.*
   d. Click *Execute Query* to create the table, views, and deletion stored procedure.
7. Use the Enterprise Manager to verify that the table, views, and deletion stored procedure was created.

8. After the objects are created successfully, if you are using SQL Server 7.0, display the Enterprise Manager, right-click *Data Transformation Services*, and select *All* tasks.
9. Click *Open Package* and browse the LT Auditor+ CD for the .dts package. Click *Open* to display the SQL Server Enterprise Manager window.

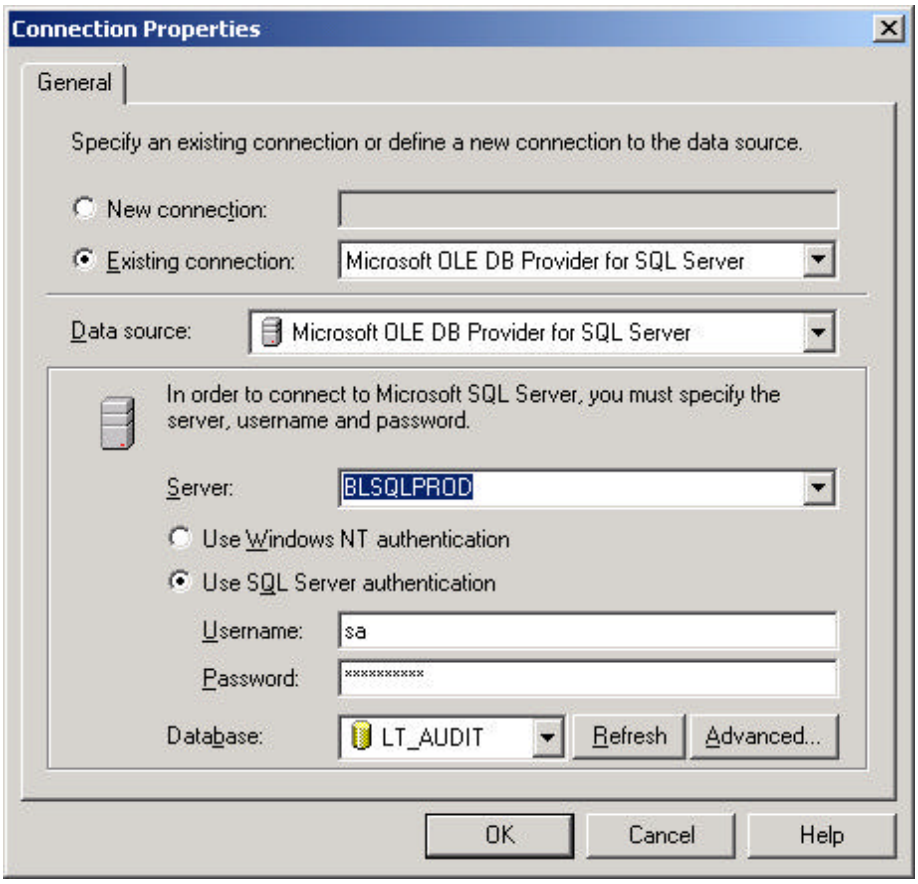


10. Double-click the server icon farthest to the left to display its Connection Properties window.



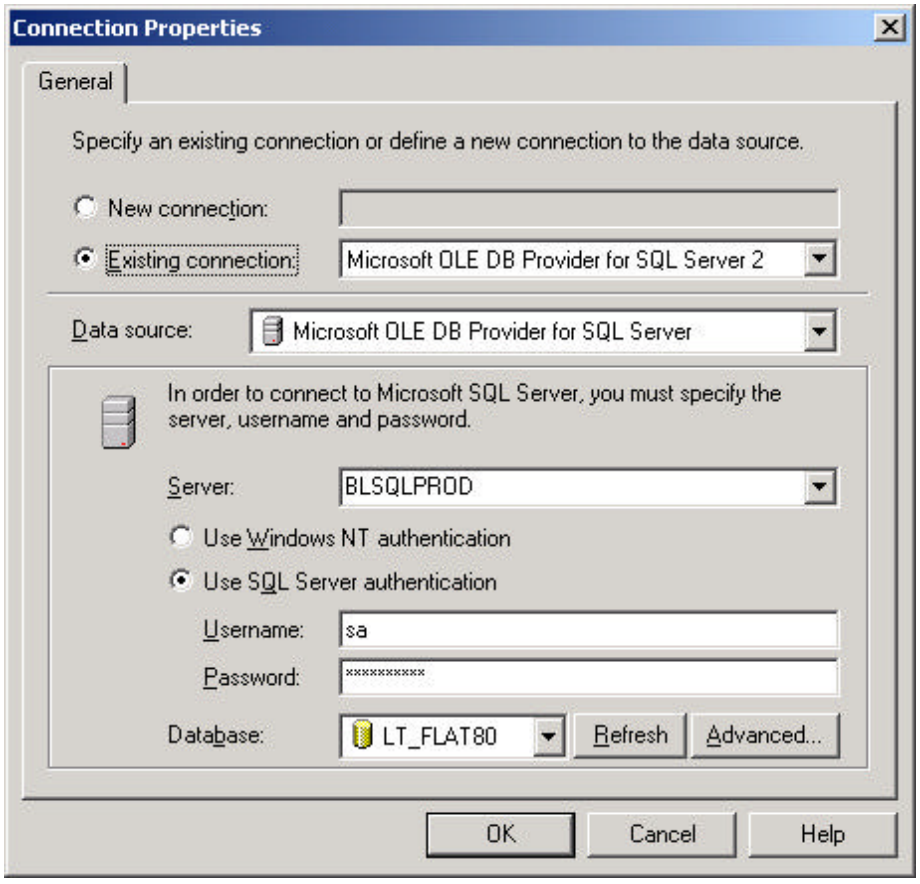
11. Modify the following information:
    - Server name to reflect the server the database was created on
    - Username and password
    - Current database

    Click *OK* to return to the SQL Server Enterprise Manager window.

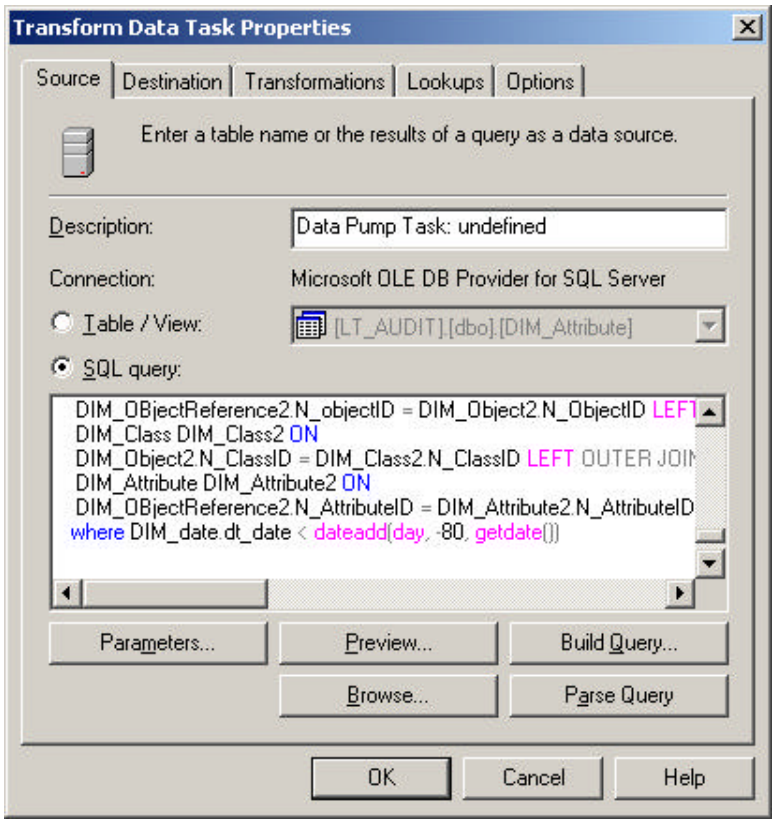


12. Double-click the server icon farthest to the right to display its Connection Properties window.
13. In the Connection Properties window, modify the following information:
    - Server name to reflect the server at the client site
    - Username and password
    - Archive database

    Click *OK* to return to the SQL Server Enterprise Manager window.

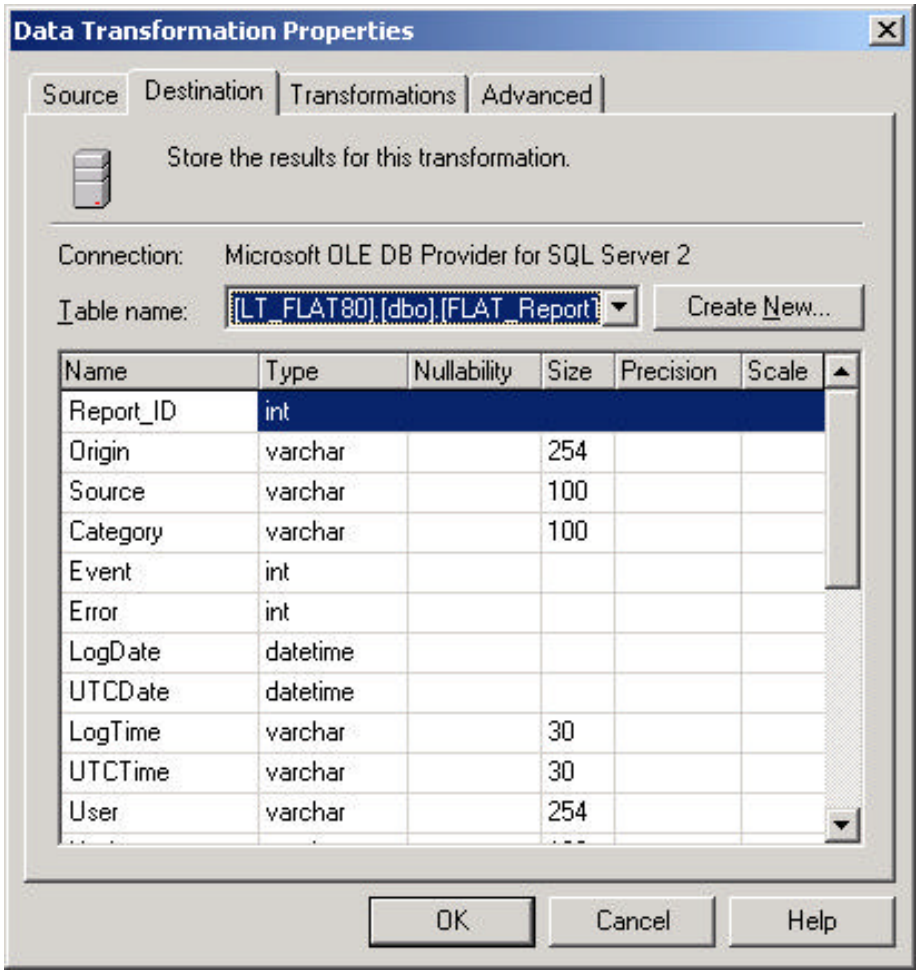


14. Right-click the arrow located between the two server icons and select *Properties*. The Transform Data Task Properties window displays.
15. In the SQL query field, use the down arrow to scroll to the end of the list box.

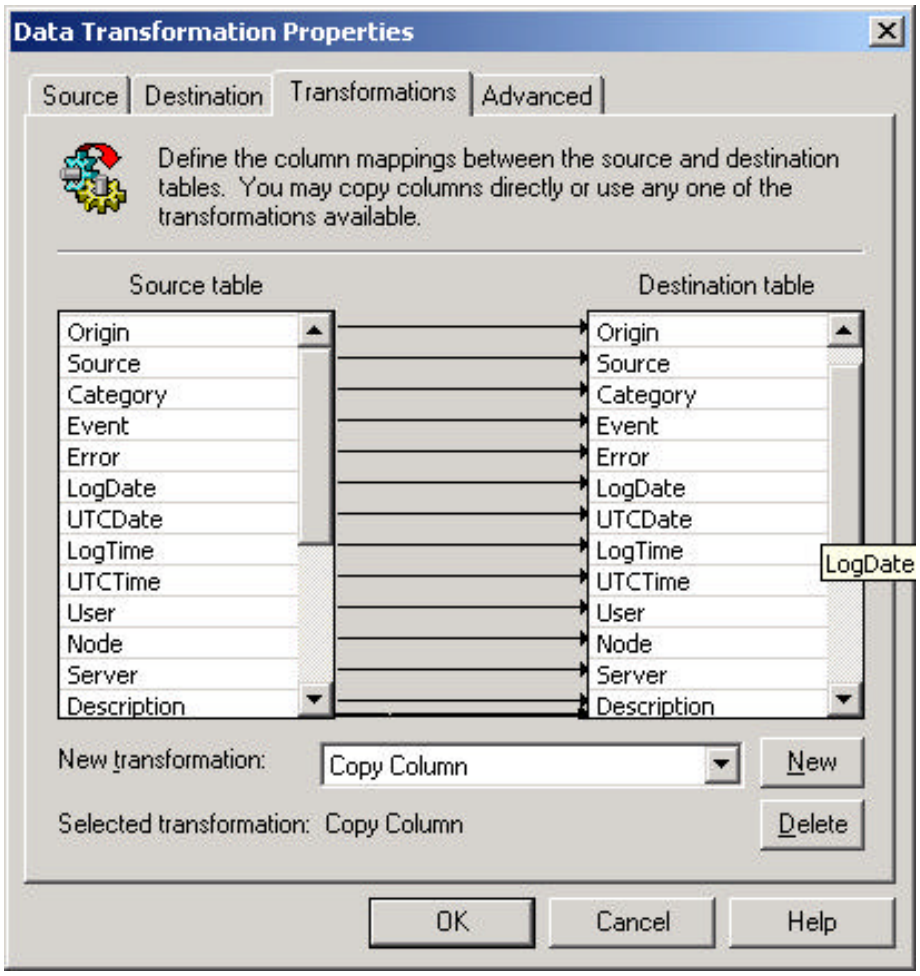


16. In the SQL query list box, the number 80 represents 80 days prior to today. Therefore, data that is older than 80 days will be archived. This number can be changed based on the your needs.

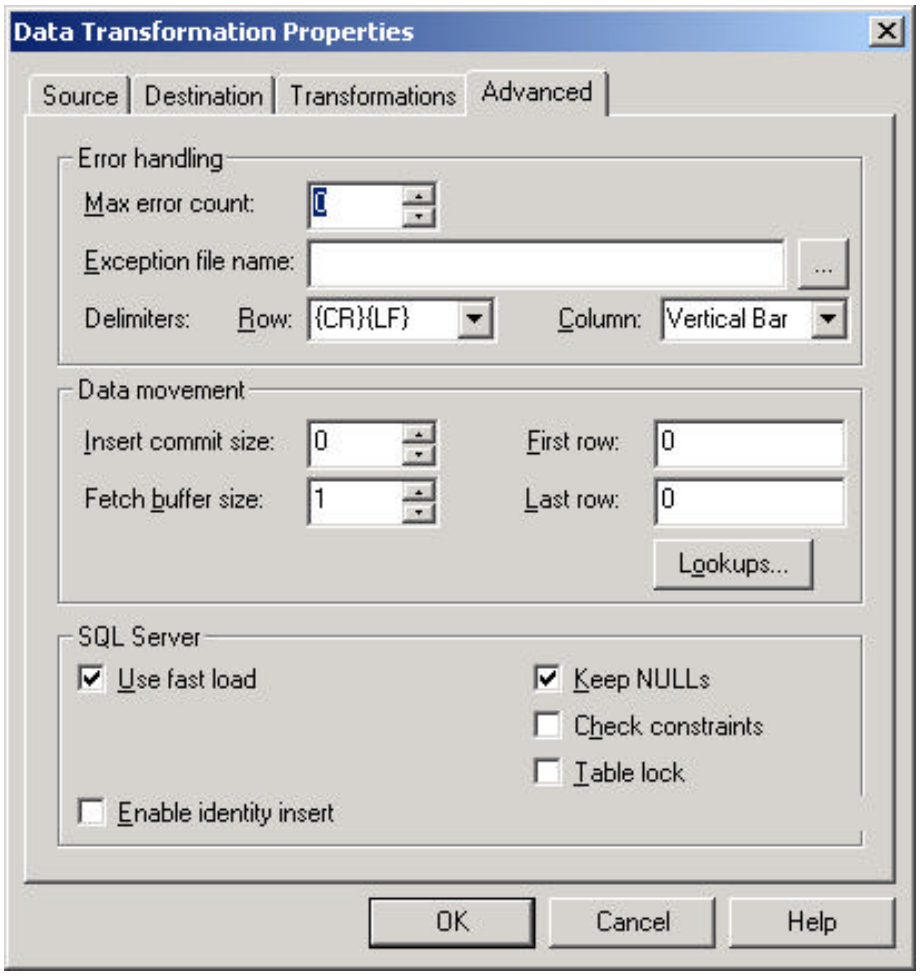
17. Click the *Destination* tab. In the Table name field, verify that the database name and table name are correct.



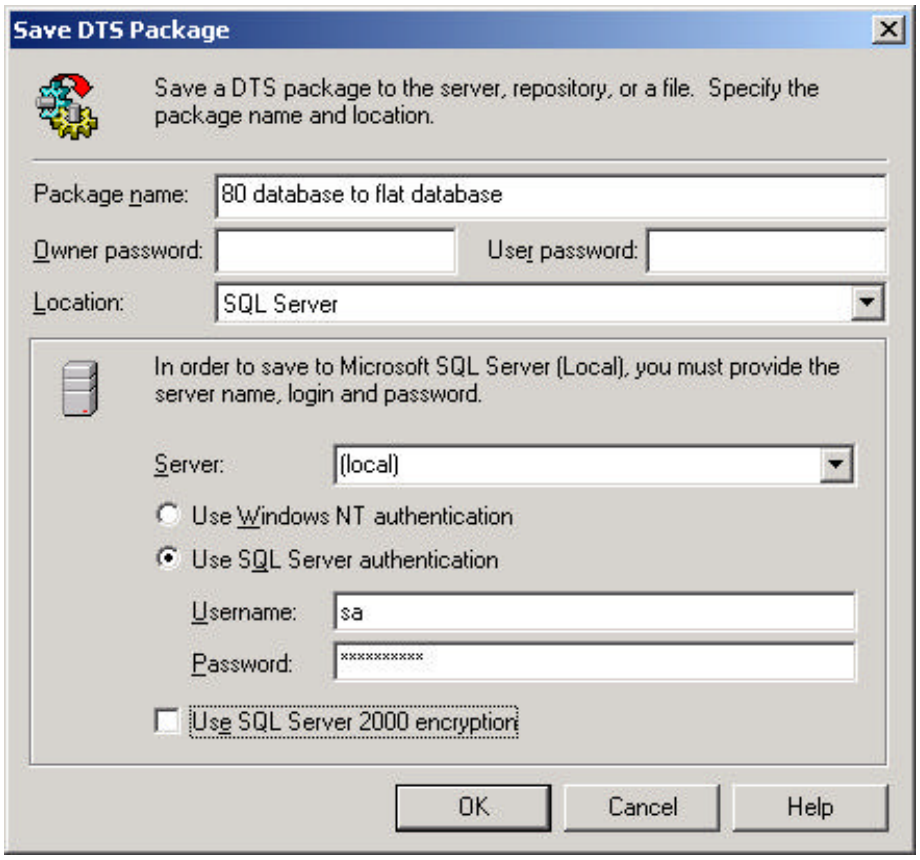
18. Click the *Transformations* tab. Verify that the Source table and the Destination table are identical.



19. Click the *Advanced* tab. In the SQL Server section, select *Use fast load and Keep Nulls*. Click *OK* to continue. Click *OK*.



20. From the Menu bar of the SQL Server Enterprise Manager window, click the package and the *Save As* button to display the Save DTS Package window.
21. Click the Location drop-down arrow and select *SQL Server*. Click the *Use SQL Server authentication* radio button and enter the username and password. Click *OK* to save the package on the SQL Server.

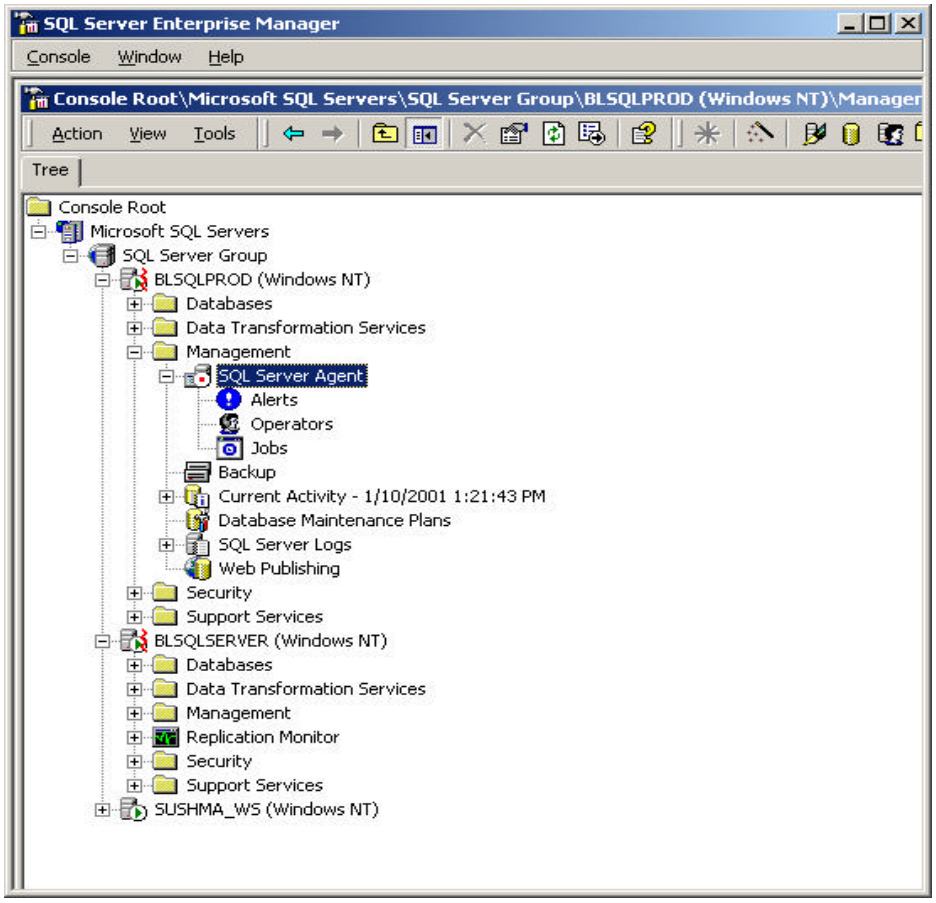


22. To schedule the package from the SQL Server Enterprise Manager window, expand the *Data Transformation Services* folder, select the local package you just saved and right-click. Click the *Schedule* button to schedule the package as a job.
23. After the DTS package is saved and scheduled, you can create a deletion job.

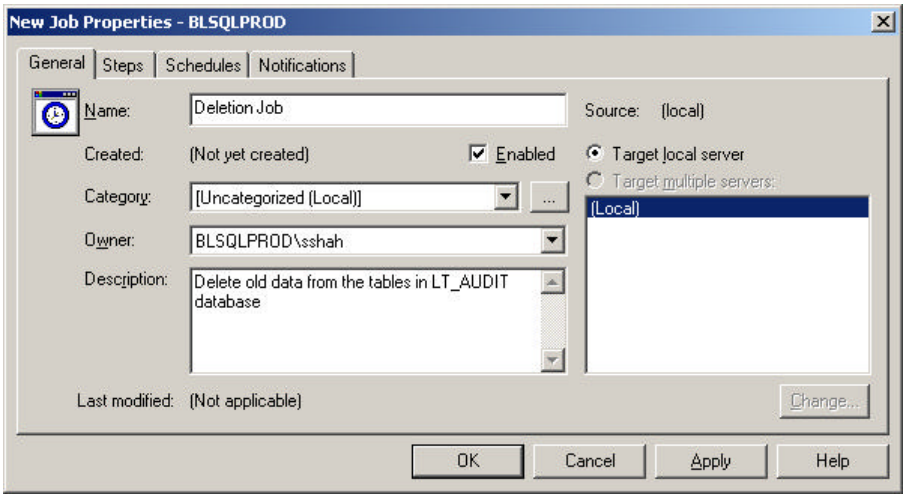
Deleting Data

To create a deletion job:

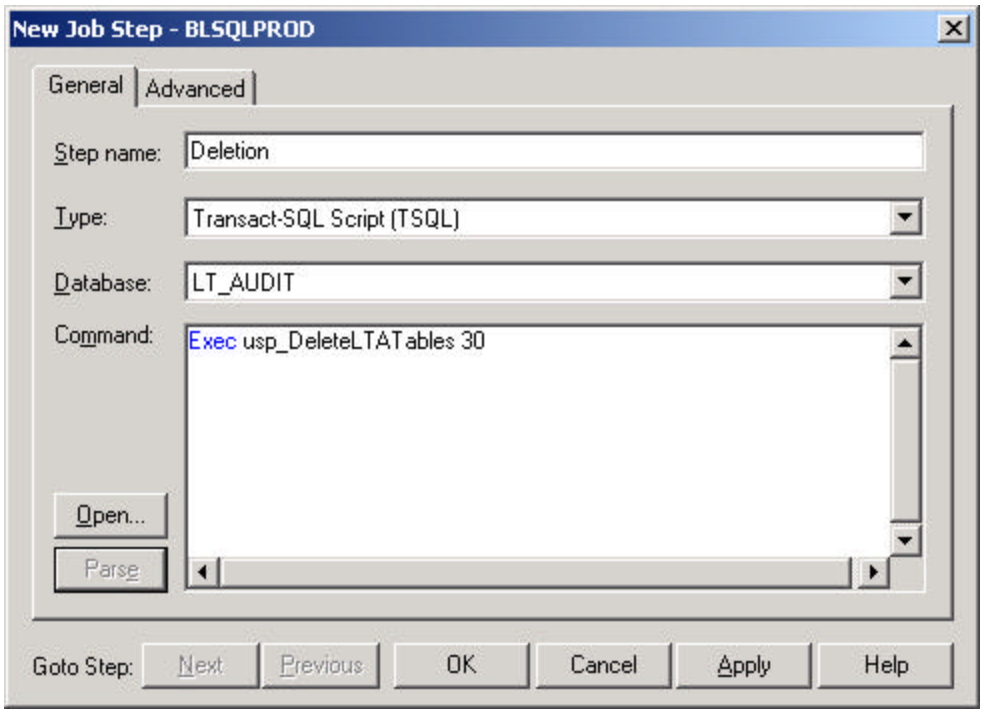
1. Click *Start* → *Programs* → *Microsoft SQL Server 7.0* → *Enterprise Manager*.
2. On the Console Root folder in the SQL Server Enterprise Manager window, expand the Management folder. Expand the *SQL Server Agent*. Right-click *Jobs* and select *New Job*.



3. From the General tab in the New Properties window, enter a name and description for your job.



4. Select the *Steps* tab and click *New*.



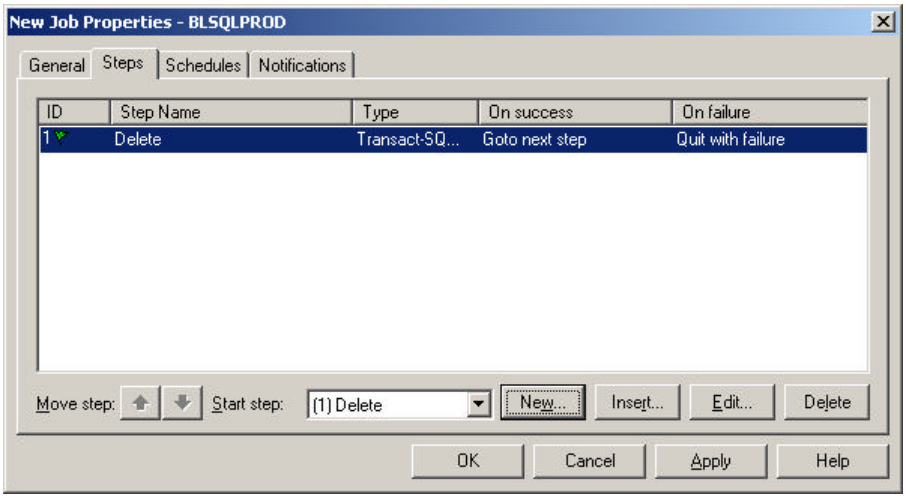
5. At the New Job Step screen, enter a name for your new job step. Click the *Type* drop-down arrow. From the drop-down menu, select *Transact-SQL Script (TSQL)*.
6. Click the *Database* drop-down arrow. From the drop-down menu, select the database from which you want to delete the data.

7. In the Command section, enter the following information:
   EXEC usp_DeleteLTATables 30

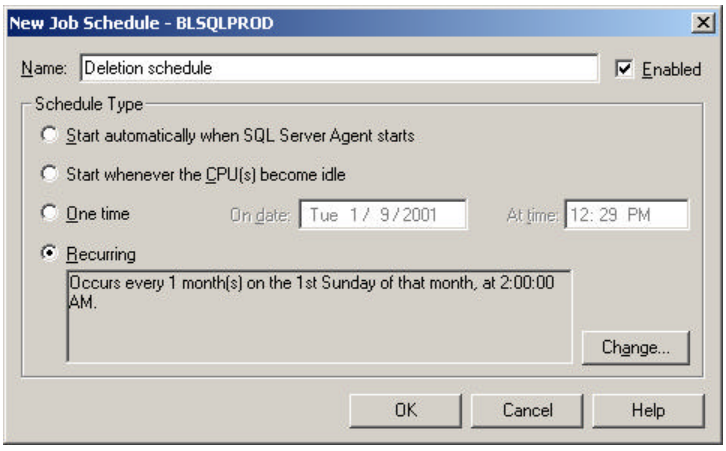
Note

The number 30 allows you to delete everything that is older than 30 days. You can customize the command by replacing the number 30.

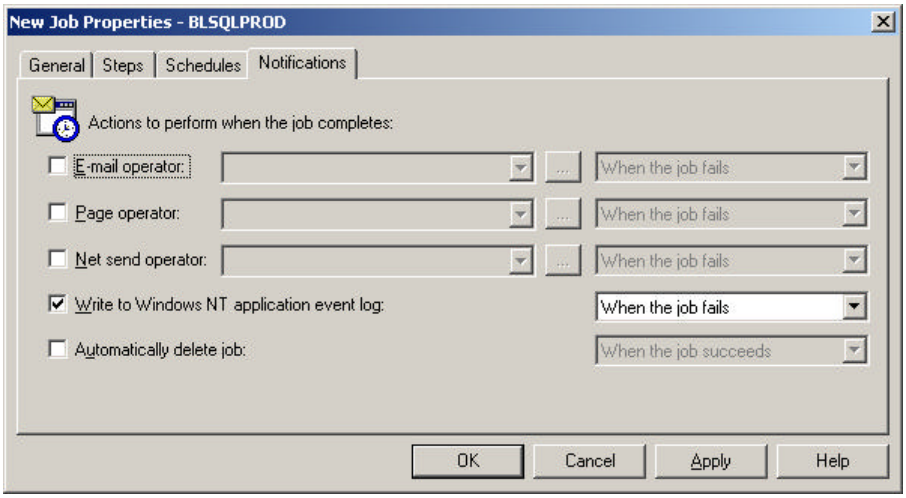
Click *OK* to save the new job step. The following screen will display confirming that the deletion job has been created.



8. Click the *Schedules* tab. Click *New* and schedule the job to automatically run once a month or as needed. Remember, to schedule the job to run during idle times. Click *OK* to exit.



9. On the New Job Properties window, click the *Notifications* tab. Use this window to modify the way in which you are notified. Click *Apply* → *OK*.



10. From the SQL Server Enterprise Manager window tree section, click *Management* → *SQL Server* → *Agent* → *Jobs*. In the right-hand pane, verify that the deletion job was created successfully.

Constructing an Oracle Database

LT Auditor+ for Windows is designed to work with Oracle 8*i* (8.1.5, 8.1.6, and 8.1.7) databases and later. Before installing Oracle (if not already installed) or setting up an Oracle database for LT Auditor+, you or your database administrator should consider reviewing the following information:

- Oracle8*i* Configuration Notes
- Oracle Net8 Configuration Notes
- Oracle Database Setup for LT Auditor+

Oracle8*i* Configuration Notes

In Oracle8*i*, the initialization parameter file is referred to as *INIT.ORA*. The file is placed in ORACLE_HOME in ADMIN\SID\PFILE. For example, if ORACLE_HOME is *D:\Oracle\Ora8i*, the *Init.ora* file will be located in the D:\Oracle\Ora8i\admin\SID\pfile directory, where SID is the instance name related to the database.

Database and Instance Name Issues

The Db_name cannot be changed after it is set. The Service_Name is set in the **Init.ora** file and corresponds to (Db_name + Domain). For example, if the Db_name is *Ltap* and the domain is *BlueLance*, the Service_Name will be *Ltap.BlueLance*.com. Oracle refers to the Service Name as the *Global Database Name*.

The Instance_Name is set in the **Init.Ora** file and instance name, which refers to the name of the Oracle database. The Instance_Name parameter links the database being started to the instance created. The Service_Name and Instance_Name are required when setting up Net8.

Java Option

If the Java Option is not installed, make sure that the Java_pool_size is set to 1 MB. If the Java_pool_size is not set to 1 MB, it defaults to 20 MB. The Java pool is an area in the System Global Area (SGA) that holds the Java libraries and classes.

If the Java Option is installed, make sure that the Java_pool_size is set to 20 MB and the Shared_pool_size is set to 50 MB.

The Oracle instance created will use the initialization parameter file that is placed in the D:\Oracle\Ora8i\Database\ folder. The file name is init<SID>.ora and is used by the Windows 2000/Windows NT service related to the instance. This file contains only one line that points to the **Init.ora** file. The password file is located in the D:\Oracle\Ora8i\Database folder.

Oracle Net8 Configuration Notes

Oracle Configuration files are located in the Oracle_home\Network\Admin\ folder. The **Listener.ora** and **Tnsnames.ora** files require the following parameters:

- **Listener.ora**
  - Global_Dbname — The Service_name used in the Init.ora file
  - Sid_Name — The Instance_Name used in the Init.ora file
- **Tnsnames.ora** — The Service_Name used in the Tnsnames.ora file

Running Oracle Scripts

Before you run Lt Auditor+ Oracle scripts, perform the following steps:

1. From the LT Auditor+ CD, copy and paste the Oracle scripts to a local folder.
2. Right-click each script and select *Properties*. Deselect the *Read Only* attribute.
3. Determine your Oracle home folder. For example, Blue Lance's home folder is C:\Oracle\Ora8i.
4. Determine where you want to create the new files. For example, Blue Lance's home folder is C:\Oracle. Blue Lance uses the following Oracle Database — SID: LTAS
5. In the following scripts, change the C: to the clients directory and replace all references of C:\Oracle to [OracleDataPath]:
   - LTASRun.SQL
   - LTASRun1.SQL
   - INITLTAS.ora
6. Setup an entry in the Tnsnames.ora file for the LTAS database.

Note

You can customize the size of the database in the following scripts:

- LTASRun.SQL
- LTASRun1.SQL

Setting Up an Entry to the Tnsnames.ora File Using Net8 Assistant

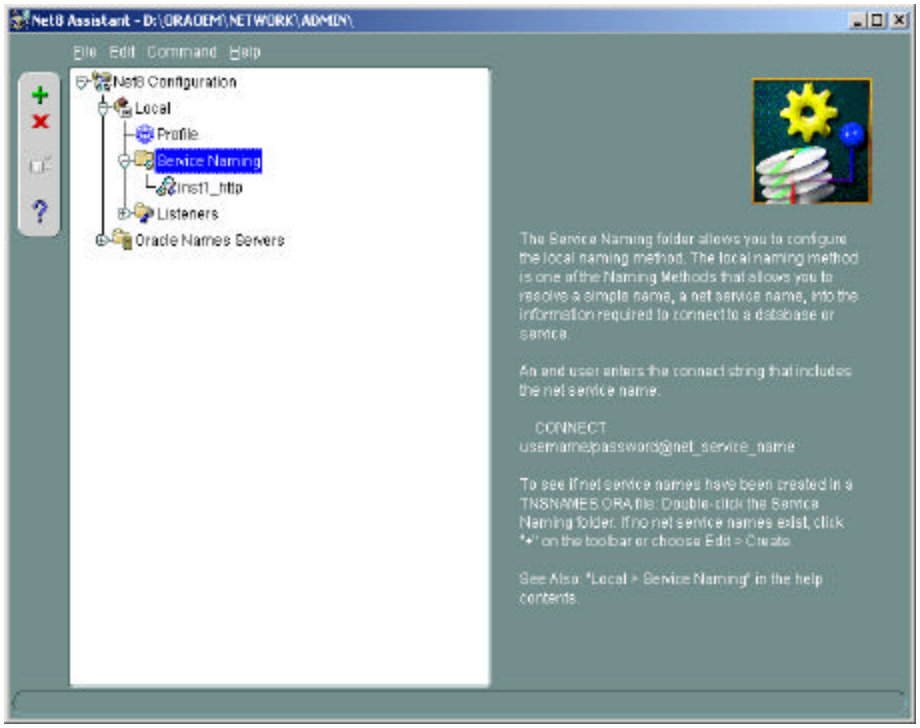
You can use Net8 Assistant to register the Oracle database and create an entry in the Tnsnames.ora file.

Note

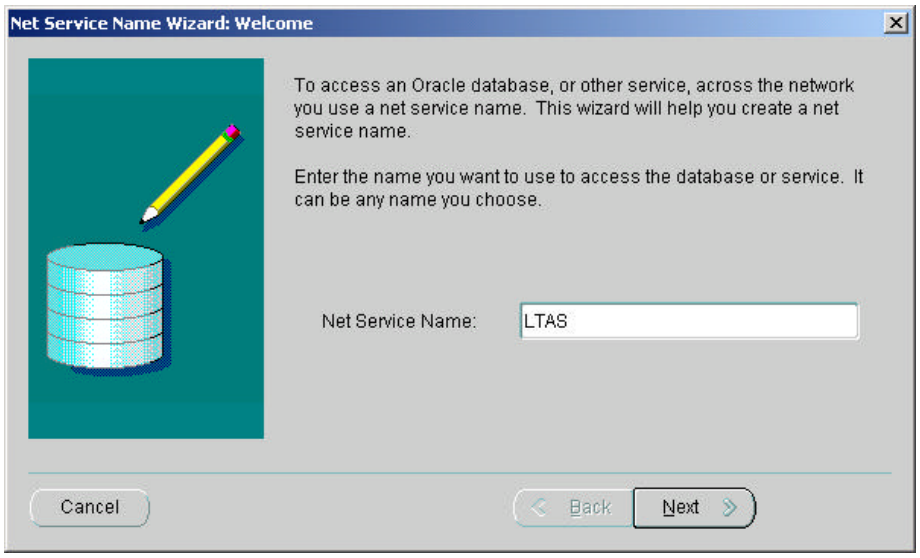
Only database administrators who are familiar with Oracle should modify the Tnsames.ora file.

To use Net8 Assistant to register the Oracle database and create an entry in the Tnsnames.ora file, perform the following steps:

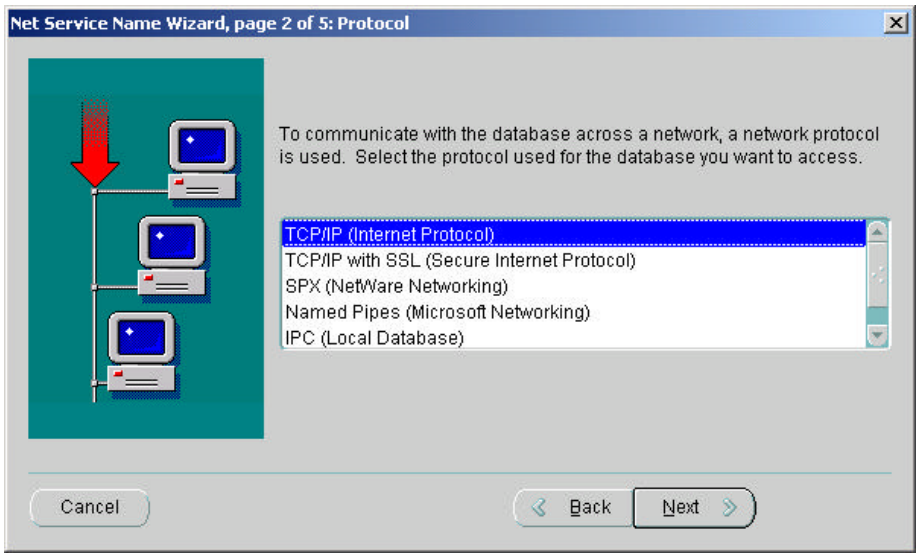
1. From Programs/Oracle /Network Administrator/ Net 8 Assistant display the Net 8 Assistant. The following window displays.


Net8 Assistant - D:\ORAOEM\NETWORK\ADMIN\
File Edit Command Help
Net8 Configuration
Local
Profile
Service Naming
inst1_http
Listeners
Oracle Names Servers
The Service Naming folder allows you to configure the local naming method. The local naming method is one of the Naming Methods that allows you to resolve a simple name, a net service name, into the information required to connect to a database or service.
An end user enters the connect string that includes the net service name.
CONNECT username/password@net_service_name
To see if net service names have been created in a TNSNAMES.ORA file: Double-click the Service Naming folder. If no net service names exist, click "+" on the toolbar or choose Edit > Create.
See Also: "Local > Service Naming" in the help contents.

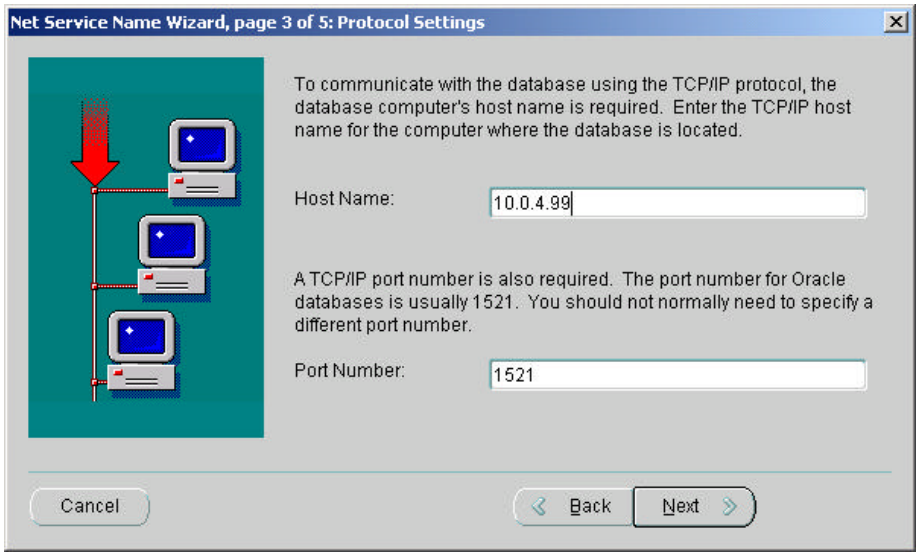
2. From the Net8 Configuration tree, expand *Local* folder and select the *Service Naming* folder.
3. Click the plus icon to display the following window.


Net Service Name Wizard: Welcome
To access an Oracle database, or other service, across the network you use a net service name. This wizard will help you create a net service name.
Enter the name you want to use to access the database or service. It can be any name you choose.
Net Service Name:
LTAS
Cancel
Back
Next

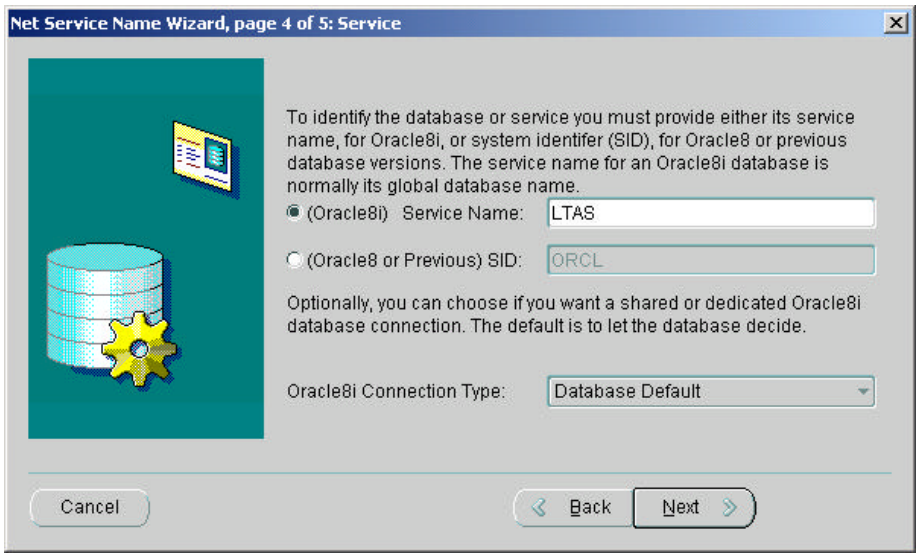
4. In the Net Service Name field, add the name of the database created for LT Auditor. Click *Next* to continue.
5. The Protocol window displays. Select *TCP/IP (Internet Protocol)*. Click Next to continue.


Net Service Name Wizard, page 2 of 5: Protocol
To communicate with the database across a network, a network protocol is used. Select the protocol used for the database you want to access.
TCP/IP (Internet Protocol)
TCP/IP with SSL (Secure Internet Protocol)
SPX (NetWare Networking)
Named Pipes (Microsoft Networking)
IPC (Local Database)
Cancel
Back
Next

6. The Protocol Settings window displays. In the Host Name field, enter the host name or the host IP where the database resides. Click *Next* to continue.


Net Service Name Wizard, page 3 of 5: Protocol Settings
To communicate with the database using the TCP/IP protocol, the database computer's host name is required. Enter the TCP/IP host name for the computer where the database is located.
Host Name:
10.0.4.99
A TCP/IP port number is also required. The port number for Oracle databases is usually 1521. You should not normally need to specify a different port number.
Port Number:
1521
Cancel
Back
Next

7. The Service window displays. Select the (Oracle 8i) Service Name radio button. In the Service name field, enter the name of the database. Click *Next* to continue.


Net Service Name Wizard, page 4 of 5: Service
To identify the database or service you must provide either its service name, for Oracle8i, or system identifer (SID), for Oracle8 or previous database versions. The service name for an Oracle8i database is normally its global database name.
(Oracle8i) Service Name:
LTAS
(Oracle8 or Previous) SID:
ORCL
Optionally, you can choose if you want a shared or dedicated Oracle8i database connection. The default is to let the database decide.
Oracle8i Connection Type:
Database Default
Cancel
Back
Next

8. The Test window displays. Click *Test* to verify your connection to the database. You will be prompted to enter the user name and password of your Oracle database. Otherwise, click *Finish* to complete the registration process. Oracle will place this entry in the TNSNames.ora file.
9. Return to the Net8 Assistant Home page and click File / Save Network Configuration to save all changes.

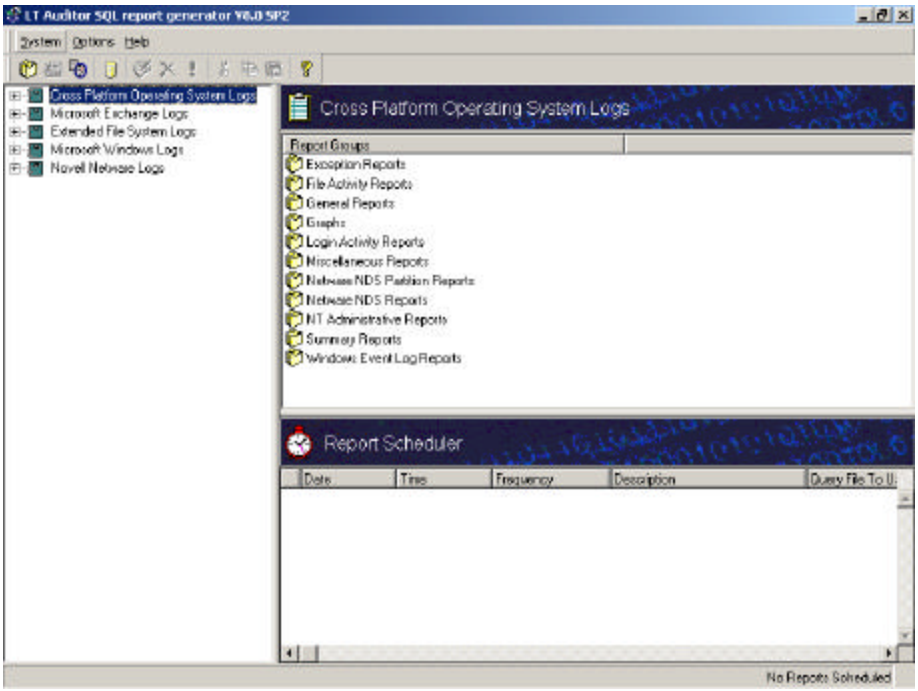
LT Auditor+ 8.0 SP2 SQL Report Generator

Chapter 4 — Using the Report Generator

Overview

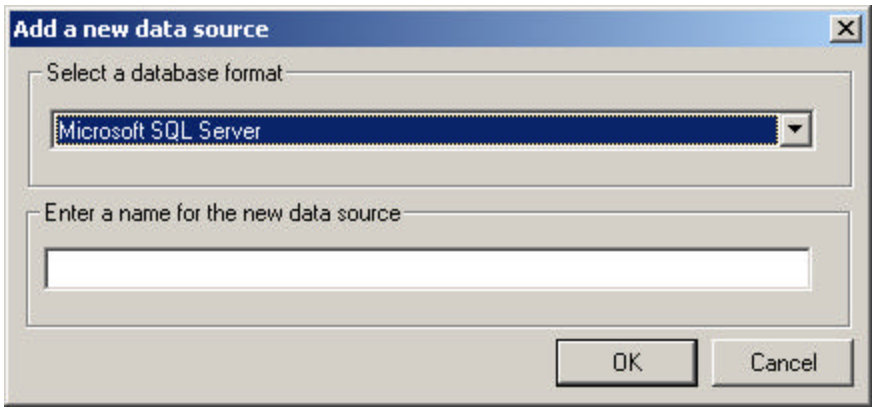
You can customize the Report Generator query function to retrieve audited data from the LT Auditor+ database and generate a report based on your criteria. These criteria can include specific events, users, error conditions, machines, and operations.

Using the Report Generator



To display the Report Generator window, click *Start* → *Programs* → *LT Auditor+* → *LT Auditor+ Report Generators* → *LT Auditor+ SQL Report Generator*.

Adding a New Data Source



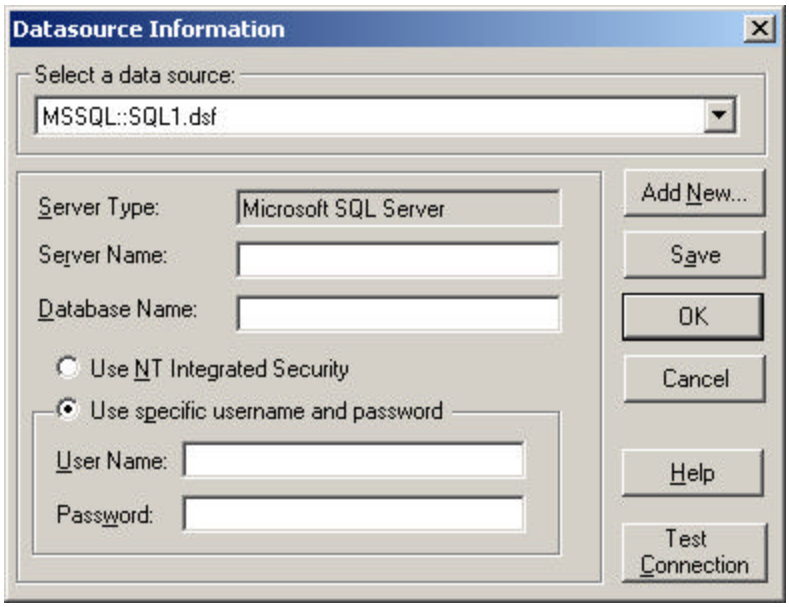
Before you can create a report query, you must select the desired database connection for the report. The Add a new data source window can be accessed using either of the following methods:

- From the *Options* menu, select *Database Connection Information*.
- From the Standard toolbar, select the *Database Connection Information* button.

From the Select a database format section, use the drop down arrow to select a Microsoft SQL Server or an Oracle database.

In the Enter a name for the new data source field, enter a name for your database. Click *OK* to display the Datasource Information window.

Microsoft SQL Server

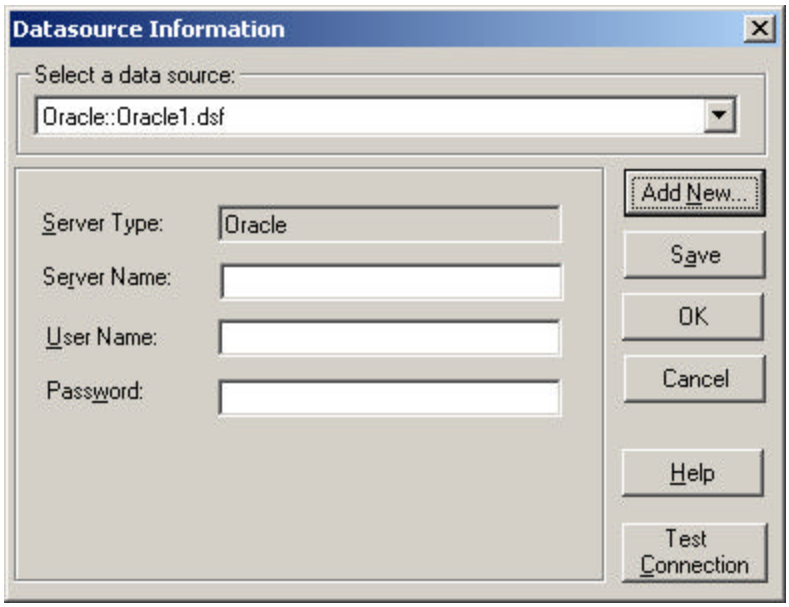


If you selected Microsoft SQL Server for your database, the preceding graphic will display. Perform the following steps to ensure that you connect to the appropriate data source file. This data source file will be used by the Report Generator to gather data for your report queries.

1. In the Server Name field, enter the SQL server name.
2. In the Database Name field, enter the SQL server database name.
3. Select either *Use NT Integrated Security* or *Use specific username and password*. If *Use specific username and password* is selected, enter the user name and password in the designated fields.
4. Click the *Test Connection* button to verify that you can connect to the selected database. Click *Save* → *OK*→ *OK* to save your changes or *Cancel* to exit without saving.

At any time you can click the *Add New* button to return to the Add a new data source window.

Oracle

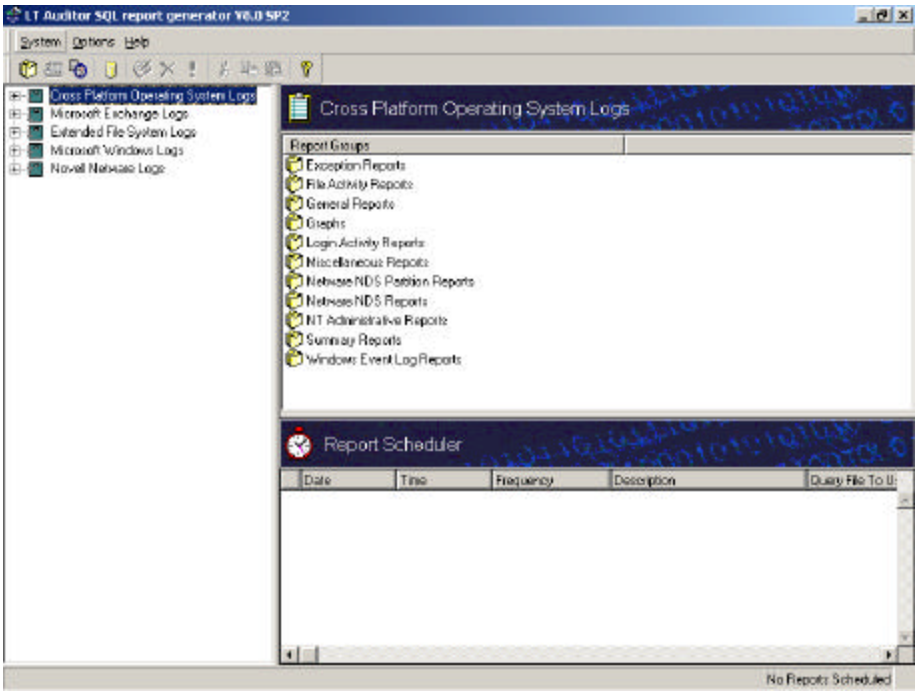


If you selected Oracle for your database, the preceding graphic will display. Perform the following steps to ensure that you connect to the appropriate data source file. This data source file will be used by the Report Generator to gather data for your report queries.

1. In the Server Name field, enter the server name.
2. Enter the user name and password in the designated fields.
3. Click the *Test Connection* button to verify that you can connect to the selected database. Click *Save* → *OK* → *OK* to save your changes or *Cancel* to exit without saving.

At any time you can click the *Add New* button to return to the Add a new data source window.

Adding a New Report Group



Using the Report Generator, you can create customized report groups and queries based on your business needs. Before adding a new report group, examine the preset report groups and queries. They may already contain the criteria for the reports you need.

Perform the following steps to add a new report group:

1. To access the Report Group window, use either of the following methods:
   - From the System menu, click *New* → *Report Group*.
   - From the Standard toolbar, click the *New Report Group* button.
2. To enter a name for the new report group, select the report group you just created and click the *Modify* button. Enter a new name for your report group and press *Enter*.

Deleting a Report Group

Perform the following steps to delete a report group:

1. From the Report Group window, highlight the desired report group you want to delete.
2. To delete the report group, use either of the following methods:
   - From the System menu, click *Delete.*
   - From the Standard toolbar, click the *Delete* button.
3. Click *Yes* to confirm the deletion of your report group.

Note
Deleting a report group will also delete all queries associated with that group.

Report Queries

Report Generator gathers and retrieves archived information from a SQL or Oracle database, then generates a report based on the criteria that define the database query. Report queries allow you to filter information concerning the network.

Report Generator ships with a variety of report queries that can be customized to fit specific criteria. In addition to modifying existing report queries, you can also create new queries for the report groups. By default, Report Generator provides several queries for each report group.

Modifying an Existing Report Query

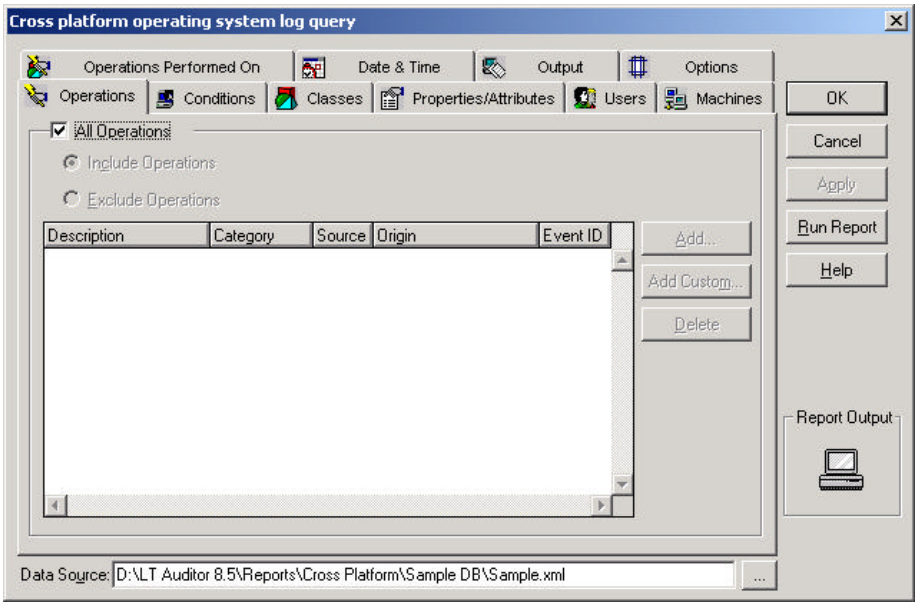
To modify an existing report query, perform the following steps:

1. From the left-hand pane of the LT Auditor+ SQL Report Generator 8.0 SP2 window, select one of the following packages:
   - Cross Platform Operating System Logs
   - Microsoft Exchange Logs(Beta)
   - Extended File System Logs
   - Microsoft Windows Logs
   - Novell NetWare Logs package
2. Highlight the desired report group to display all report queries that are part of the selected group.
3. Highlight the desired report query.
4. To display the report query window, use any of the following methods:
   - From the System menu, click *Modify.*
   - From the Standard toolbar, click *Modify.*
5. Select a tab to customize the criteria for your query.
6. Click *Apply* → *OK* to save your query or click *Run Report*. Run Report is the physical act of running a query to retrieve an output. Report Output is the output type selected, such as .doc, and .txt

Note

At any time during the report query process, you can choose to save the query, cancel the process, apply, or run a report. You do not have to use all the tabs in order to form a query.

Cross Platform Operating System Log Query Window



If you select a query from a group in the Cross Platform Operating System, Microsoft Windows Logs, or the Novell NetWare Logs package, the preceding window displays.

This window consists of the following tabs:

- Operations
- Conditions
- Classes
- Properties/Attributes
- Users
- Machines
- Events Performed On
- Date & Time
- Output
- Options

Operations Tab

Use the Operations tab to identify the network operations to be used in your query. An **operation** is an event that is audited by LT Auditor+.

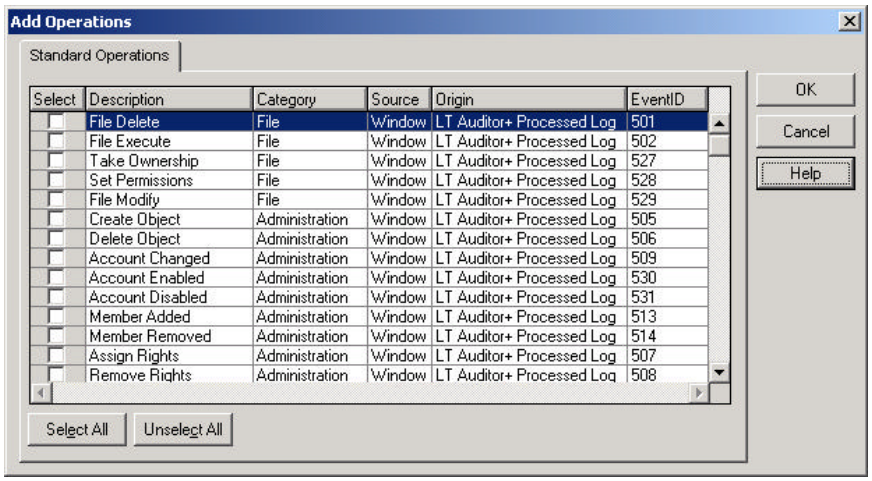
From the Operations tab, select one of the following options:

- **All Operations** — Includes all operations in your query.
- **Include Operations** — Displays operations that are generated by the event log.
- **Exclude Operations** — Displays all records that **do not** match the operations you select.

Including or Excluding Operations

Perform these steps to select certain operations to include or exclude in your query:

1. From the Operations tab, deselect the *All Operations* box and select the *Include Operations* or *Exclude Operations* button.
2. Click *Add* to display the Add Operations window.

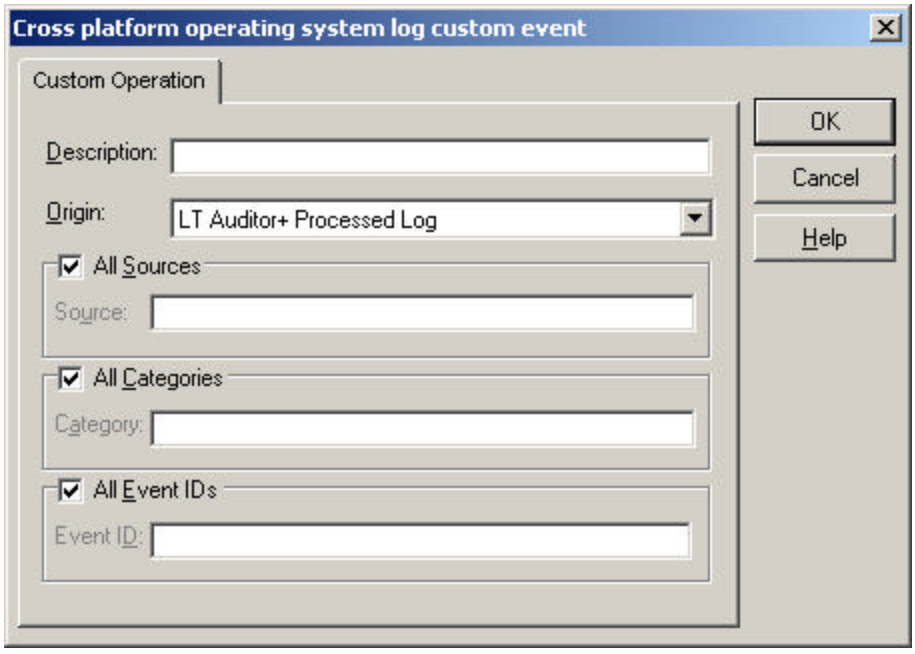

Add Operations
Standard Operations
Select
Description
Category
Source
Origin
EventID
File Delete File Window LT Auditor+ Processed Log 501
File Execute File Window LT Auditor+ Processed Log 502
Take Ownership File Window LT Auditor+ Processed Log 527
Set Permissions File Window LT Auditor+ Processed Log 528
File Modify File Window LT Auditor+ Processed Log 529
Create Object Administration Window LT Auditor+ Processed Log 505
Delete Object Administration Window LT Auditor+ Processed Log 506
Account Changed Administration Window LT Auditor+ Processed Log 509
Account Enabled Administration Window LT Auditor+ Processed Log 530
Account Disabled Administration Window LT Auditor+ Processed Log 531
Member Added Administration Window LT Auditor+ Processed Log 513
Member Removed Administration Window LT Auditor+ Processed Log 514
Assign Rights Administration Window LT Auditor+ Processed Log 507
Remove Rights Administration Window LT Auditor+ Processed Log 508
OK
Cancel
Help
Select All
Unselect All

3. From the Standard Operations tab, select the desired operation by clicking the *Select* box next to the operation. To choose all the operations, click the *Select All* button.

4. Click *OK* to save your selections and display them in the Operations tab window.

5. From the Operations tab, click the *Conditions* tab to select more criteria for your query. Then click *Apply* → *OK* to save your query or click *Run Report*. Run Report is the physical act of running a query to retrieve an output. Report Output is the output type selected, such as .doc, and .txt.

Creating Custom Operations



Using the Custom Operation feature, you can search for specific sources, categories, and event IDs. The information for each of the custom operation fields, except origin, can be found in the event logs.

Perform the following steps to add a custom operation to your standard operations list:

1. From the Operations tab window, deselect the *All Events* check box.
2. Click *Add Custom* to display the Custom Operation window.
2. Click *Add* to open the Cross platform operating system log custom event window.
3. Enter a description for the operation.
4. Use the Origin drop-down menu to select an event log.

5. In the remaining three fields — Source, Category, and Event ID — either leave all the boxes checked or enter a description for the fields.

> **Note**
> At least one of the three fields needs to be populated in order for the custom operation feature to work.

6. Click *OK* to save the new operation.
7. From the Add Custom Operations window, select the newly created custom operation and click *OK*.
8. From the Operations tab, click the *Conditions* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

> **Important**
> The Add Custom feature is not available in the Microsoft Exchange Logs and Extended File System Logs packages

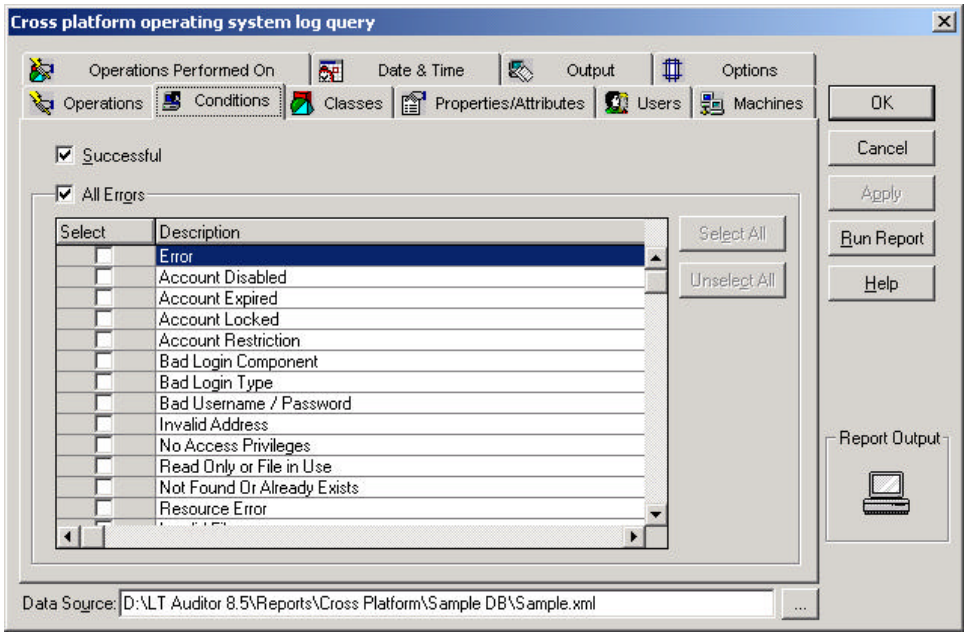
Deleting Operations

Perform the following steps to delete an operation from your query.

1. From the Operations tab, highlight the desired operation.
2. Click *Delete.* Click *Yes* to confirm the deletion. The operation is removed from the report query.

> **Note**
> If you delete a custom operation from the operation list, the operation is permanently deleted.

Conditions Tab



A **condition** is any action that occurs only if a specific circumstance is met.

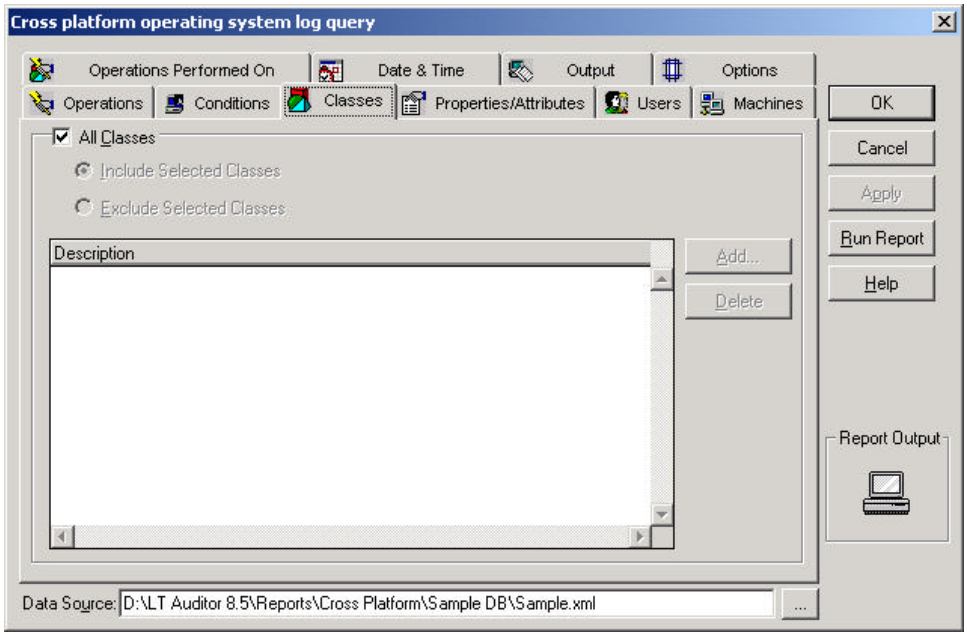
Use the following steps to add conditions to your query.

1. By default on a new report query, the *Successful* and *All Errors* check boxes are selected. To select a specific error, deselect the *Successful* and *All Errors* check boxes.

> **Note**
> Checking *All Errors* prevents you from selecting specific conditions, such as error, account disabled, or invalid address. Therefore, if you check *All Errors*, you must move to the next tab or save the query.

2. Select the desired conditions or click the *Select All* button.
3. From the Conditions tab, click the *Classes* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

Classes Tab



A **class** is a template or blueprint that defines the characteristics of an object and describes how the object should look and behave.

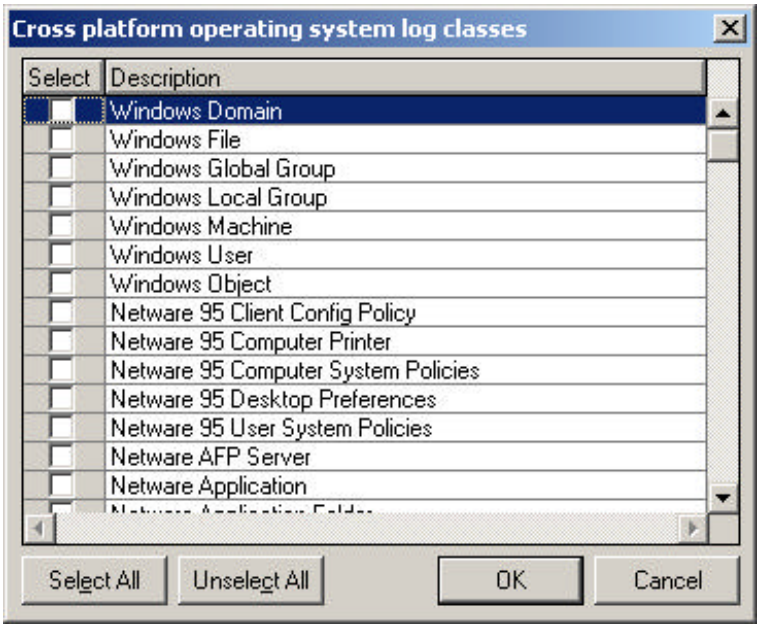
Example

An administrator creates a group called *Marketing*. In the system, **group** is the class and **Marketing** is the object.

Perform the following steps to add a class to your query:

1. Check the *All Classes* box to include all available classes in the query. Otherwise, click *Include Selected Classes* to report on selected classes. Click *Exclude Selected Classes* to report on all classes **other** than those selected in the Classes tab.

2. Click *Add* to include a class in your query. The Cross platform operating system log classes window displays.

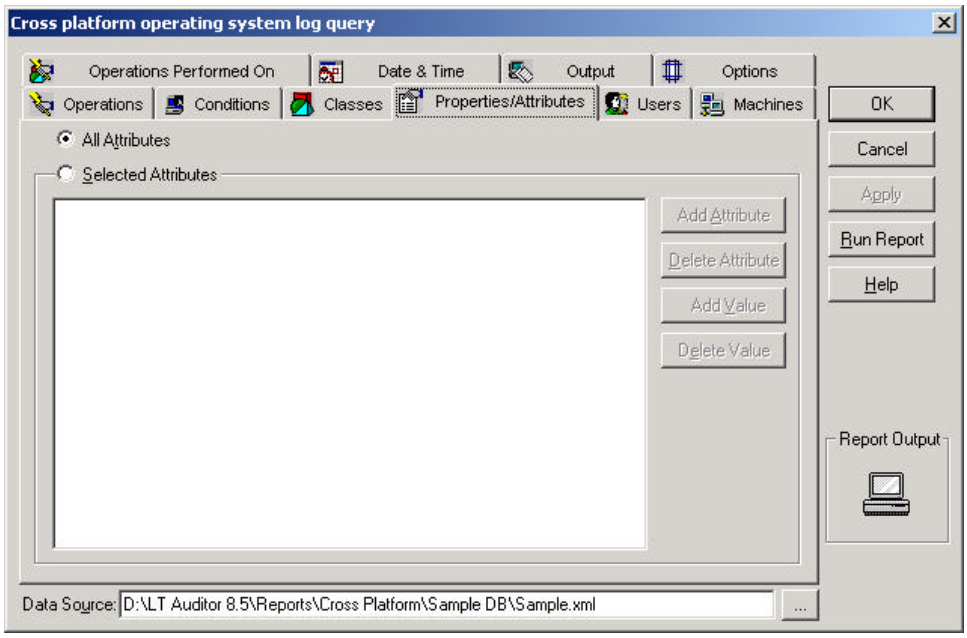


3. Select the desired classes by clicking the appropriate box in the Select column or click *Select All*.

4. Click *OK* to save your selections and return to the Classes tab window.

5. In the report query window, click the *Properties/Attributes* tab to select more criteria for your query, click *Apply* →*OK* to save your query, or click *Run Report*.

Properties/Attributes Tab



Properties or **attributes** indicate one or more characteristics of an object.

Example

Attributes of a user include:

- Full name
- Password
- Member of:

Attributes of a group include:

- Descriptions
- Members

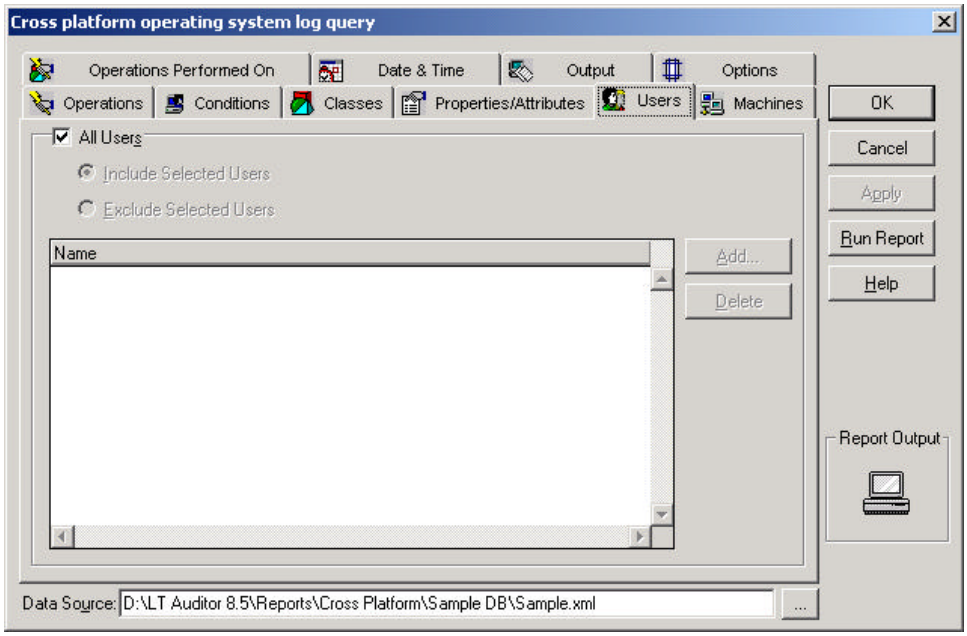
Use the Properties/Attributes tab to add specific properties and attributes to your query:

- **All Attributes** — Queries for all attributes
- **Selected Attributes** — Adds specific attributes to your query
- **Add Attribute** — Adds specific attributes to include in your report
- **Delete Attribute** — Deletes specific attributes from the list
- **Add Value** — Adds a new attribute value for the selected attribute
- **Delete Value** — Deletes the selected attribute values from the list

Perform the following steps to add an attribute:

1. Click the *Selected Attributes* radio button.
2. Click *Add Attribute.*
3. Enter the attribute name and click *OK*. The Properties/Attributes tab displays.
4. In the report query window, click the *Users* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

Users Tab



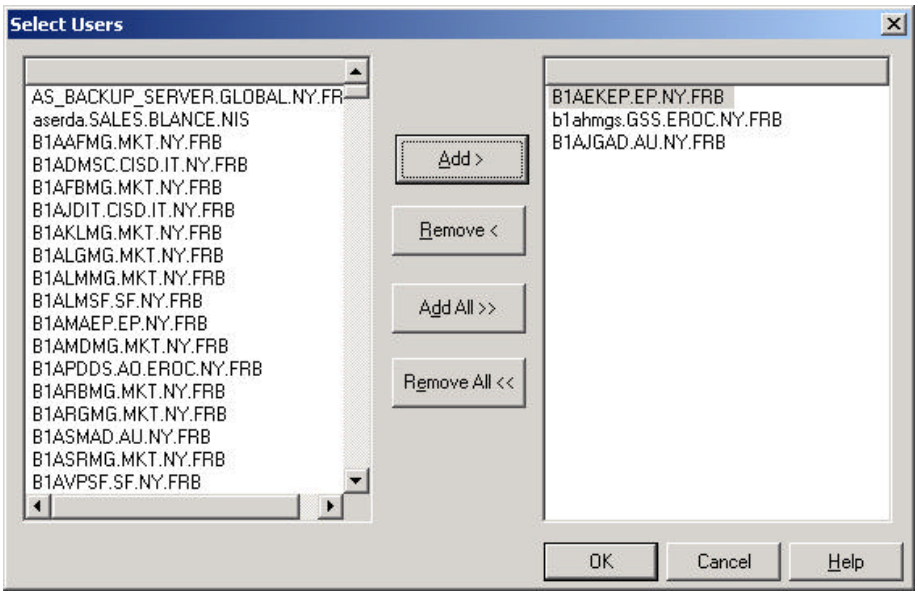
Select the Users tab to query specific users.

1. Check the *All Users* box to query all users within the network, or deselect the box to query selected users.
2. Click *Include Selected Users* to report on selected users, or click *Exclude Selected Users* to report all users other than those selected in the Users tab.

3. Click *Add* to add a specific user to the query and to display the Add a user window.

   a. Enter the name of the user you want to include in your query or click the *Browse* button. If you enter the user name, you must use the full syntax. For Windows NT, enter *domain\username.* For NetWare, enter *username.context*. Select the desired user from the list provided.

      If you click *Browse* the following window will display.



      Select a user name and click *Add*.

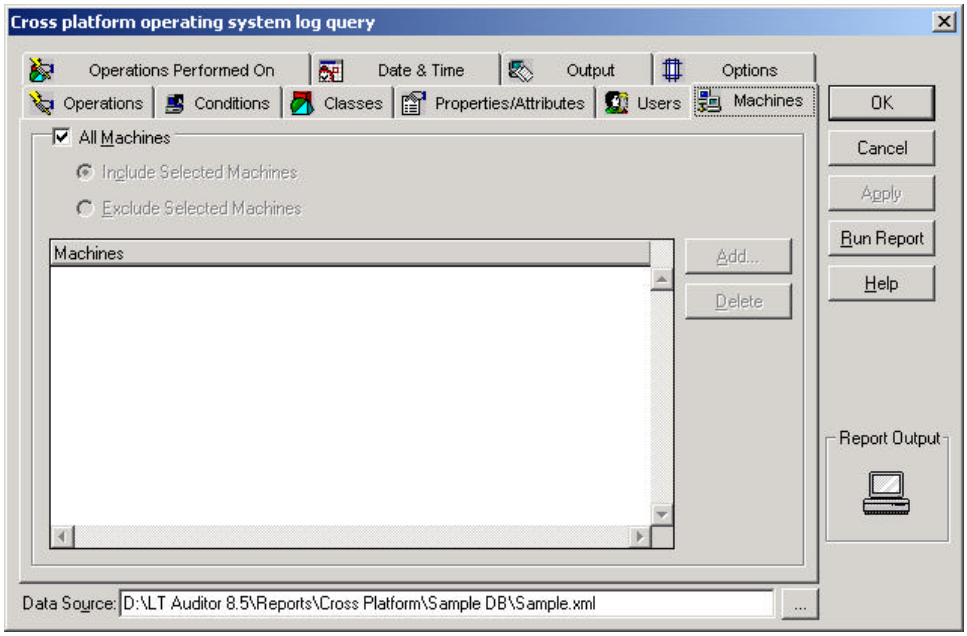
   b. Click *OK* to save your changes and display the Add a user window.

   c. Click *OK* to include the user name in your query and display the Users tab window.

4. Click *Delete* to remove the selected user from the query.

5. In the report query window, click the *Machines* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

Machines Tab



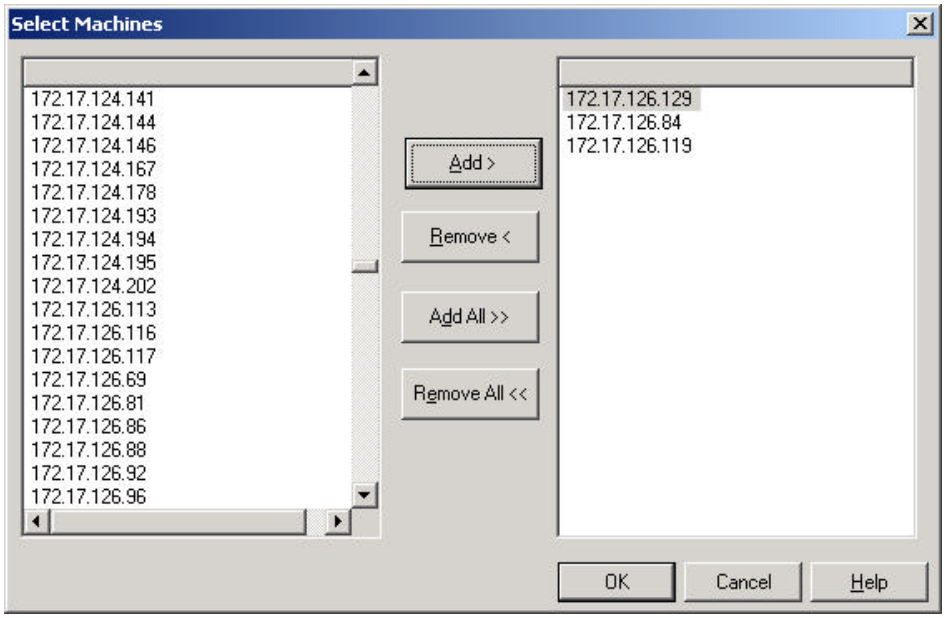
Use the Machines tab to include certain network computers in your query. This tab displays IP addresses, MAC addresses, and machine names.

Note
A machine can be a workstation, fax, or any other machine connected to the network.

1. Deselect the *All Machines* box to query available computers in the network, or deselect the box and click either *Include Selected Machines or Exclude Selected Machines.*

2. Click *Add* to display the Add a machine window.

   a. Click the *Browse* button to select a computer. The following window displays.



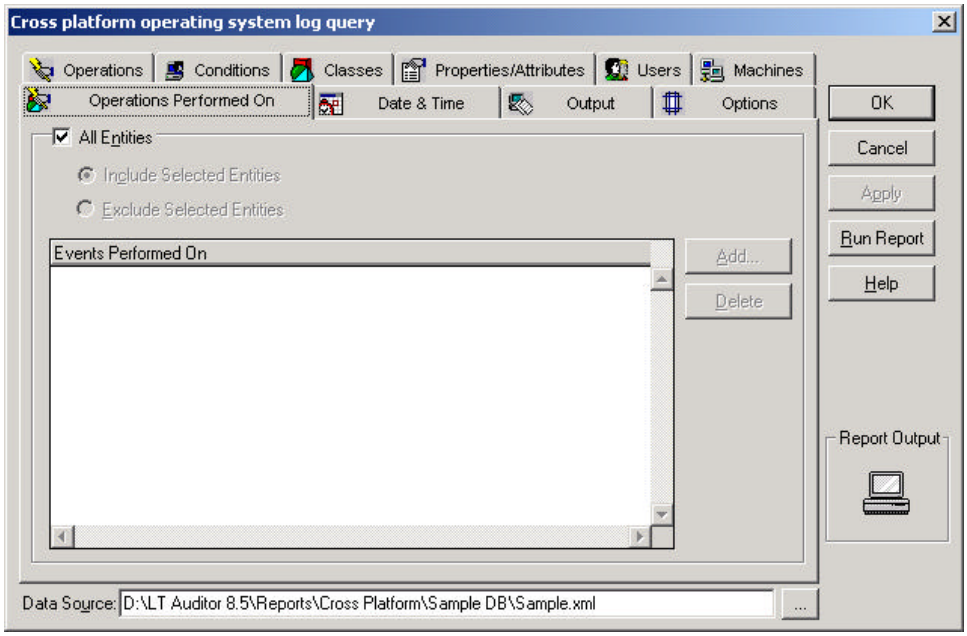
   b. Select a computer name and click *Add* → *OK* to return to the Add a machine window.

   c. Click *OK* save your changes and display the Machines tab window.

3. If you want to delete a machine from your query, highlight the desired machine name located in the Machines tab window. Click *Delete.* The machine is removed from the list.

4. In the report query window, click the *Operations Performed On* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

Operations Performed On Tab

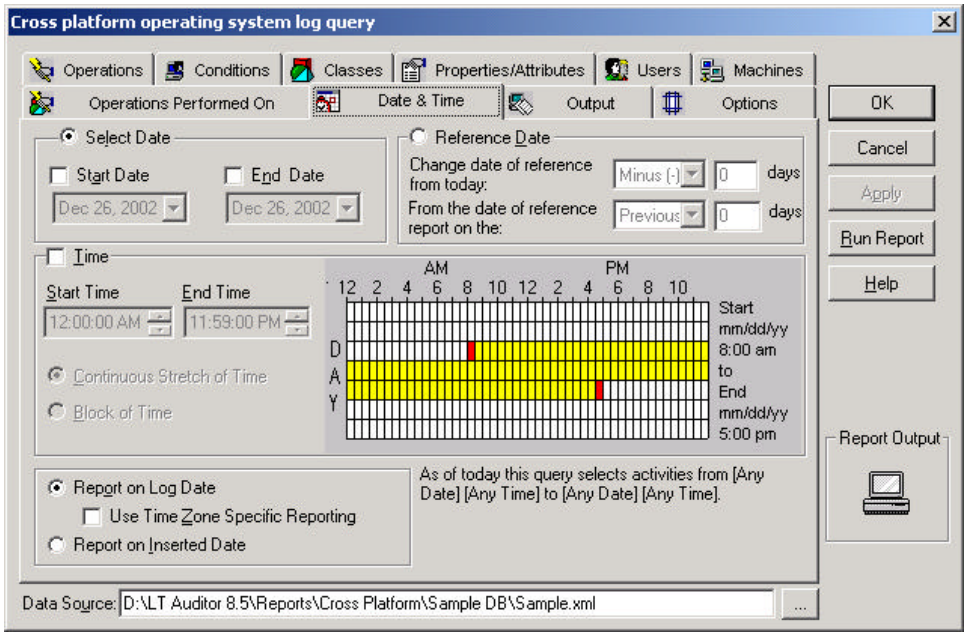


An **entity** is an object on which you can perform an operation, such as a file, another user, or machine.

By default the *All Entities* option is checked. Deselect *All Entities* to query the selected entities.

1. Click *Include Selected Entities to* report on selected Operations Performed On entities, or click *Exclude Selected Entities* to report all entities other than those listed in the Events Performed On tab.
2. Deselect *All Entities* and click *Add* to open the Add Operation Performed on Entity window.
3. In the Entity Name filed, enter the name of the file, user, or machine you would like to query. Click *OK*. The newly added entity displays in the Events Performed On column.
4. In the report query window, click the *Date & Time* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

Date & Time Tab



Use this tab to specify a date and time range for the data to be included in the report. On the Date & Time tab, you have the following options, which you can access by clicking the radio button above the desired option:

- Use the Select Date option to set a specific start date and end date to run a report. To run this same report for a different set of dates, you must enter new dates in the Start Date and End Date fields.
- Use the Reference Date option to run reports based on their relationship to the current date. Because the system automatically updates the current date, you can set the report query to run many times on different dates. Each time the report runs, the Start Date and End Date will recalculate based on the Reference Date.

Example

To run reports in scheduled mode such as daily reports, modify the Date & Time tab as follows:

1. Select the *Reference Date* radio button. This tells you from which date the calculation will be performed. To use the current date:
   a. From the Change date of reference from today drop-down menu, select Minus (-).
   b. In the day field, enter *0*.

Note
0 represents the current day. Negative numbers represent days in the past. Positive numbers represent days in the future.

   c. By default, reports on all activities will be monitored from 12:00:00 A.M. to 11:59:59 P.M.

2. Based on your reporting requirements, select the *Report on Log Date* or *Report on Inserted Date* radio button.

- Use the Time option to select the Start Time and End Time for the report. You can also run the report for either a specific block of time or a continuous stretch of time. The following time options are available:
  - Start Time/End Time — Determines the starting and ending time for the report.
  - Continuous Stretch of Time — Reports on all activities within the defined date time range.
  - Block of Time — Reports on all activities within the defined date range, which falls inside the block of time range.

- Select the Report on Log Date radio button for a report of activities captured at the specified log date and time. The log date is the date and time when an event was actually captured.
  - Use Time Zone Specific Reporting — Reports on all activities occurring at the specified date and time in a certain time zone.
- Select the Report on Inserted Date radio button to report on activities occurring when logs were inserted into a SQL server database. This report is not affected by time zones.

  Example

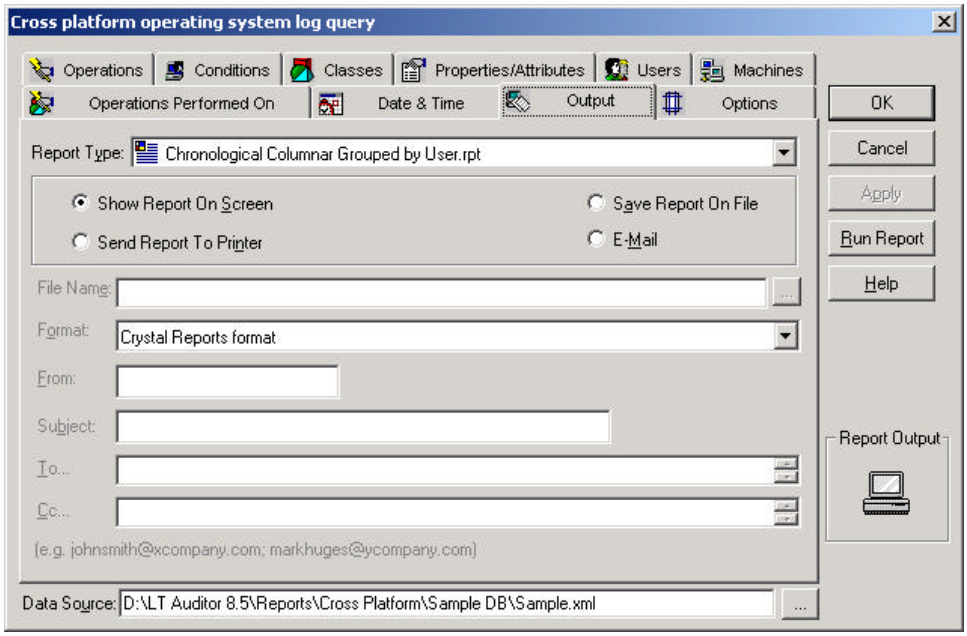
  An administrator is auditing a machine located in New York, so the events are being logged in Eastern Standard Time (EST).

  User A deletes a file at 10:00 AM (EST). A group of log files are consolidated into a SQL Server database in Houston at 1:00 PM Central Standard Time (CST). EST is the time zone specified for the report.

  The Log Date is 10:00 AM.

  The Report On Inserted Date is 1:00 PM.

Output Tab



Use the Output tab to specify how and where your report is displayed.

1. Click the drop-down arrow in the Report Type field to select a report type. This list displays all possible report types, including detailed reports, summary reports, and graphs.
2. Select a report output by clicking the desired radio button:
   - Show Report On Screen — Displays the report to screen.
   - Send Report To Printer — Generates the report directly to the default printer.
   - Save Report On File — Exports the report to a file or to another disk media.
   - E-Mail — Sends an exported report to SMTP e-mail address.

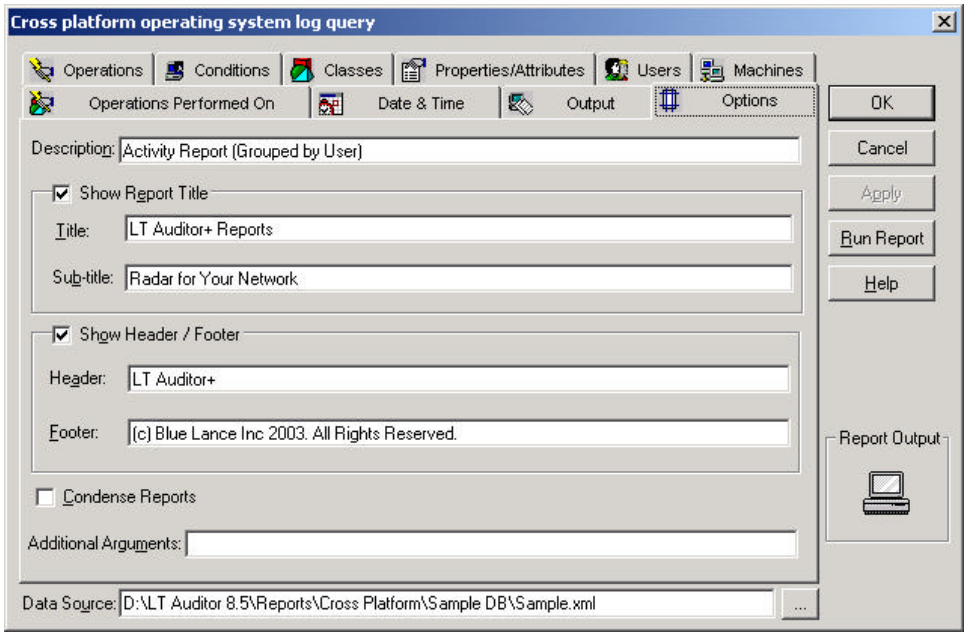
   Note
   Ensure that SMTP parameters are set properly for delivery of mail. See the SMTP options section on the LT Auditor+ Console.
3. Enter a file name to specify a destination for the report file. This is required when saving reports to a file or when e-mailing reports.

4. Click the drop-down arrow to select a format for the report. The list contains possible export formats. Selecting an export format is required when saving reports to a file or when e-mailing reports.

5. Designate an e-mail address where the report will be sent by entering the address into the To and the optional CC field. Ensure that the correct e-mail address has been entered, because Report Generator does not validate this information.

6. Click the *Options* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

Options Tab



Perform the following steps to add specific details to your query, which will be displayed in the report output.

1. Enter a description that defines this query.
2. Check the *Show Report Title* box to display the title and subtitle on the report.
   a. Title — Enter a title to display in the report.
   b. Subtitle — Enter a subtitle to display in the report.
3. Check the *Show Header/Footer* box to show a report header and footer in the report, which will appear on each page of the report.
   a. Header — Enter a header to display in the report.
   b. Footer — Enter a footer to display in the report.

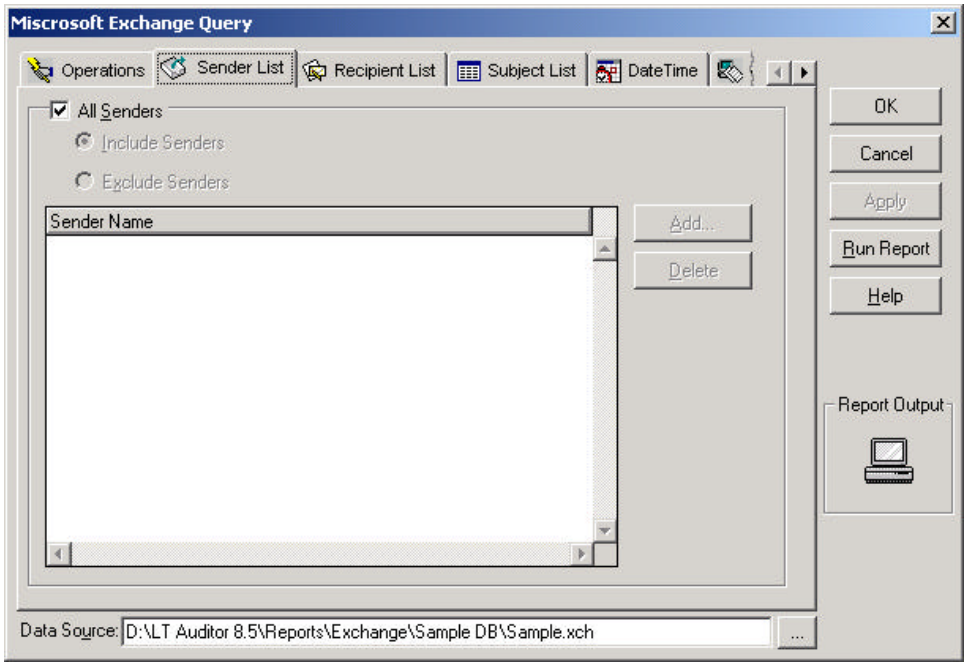
4. Check the *Condense Reports* box to condense reports that contain large amounts of data and information. Reports of major activities usually contain multiple activities performed on the operating system that are not essential for a report. When reports are condensed, some events are not shown.

   Example

   When a user is created, default attributes are set for that user. This creates additional events in the database. You can suppress these additional events by checking the *Condense Reports* option.

5. Use the Additional Arguments option to specify additional arguments for the report. Arguments can be specified to display reports with specific conditions.

Microsoft Exchange Query Window



If you select a query from a group in the Microsoft Log Report Query package, the preceding window displays.

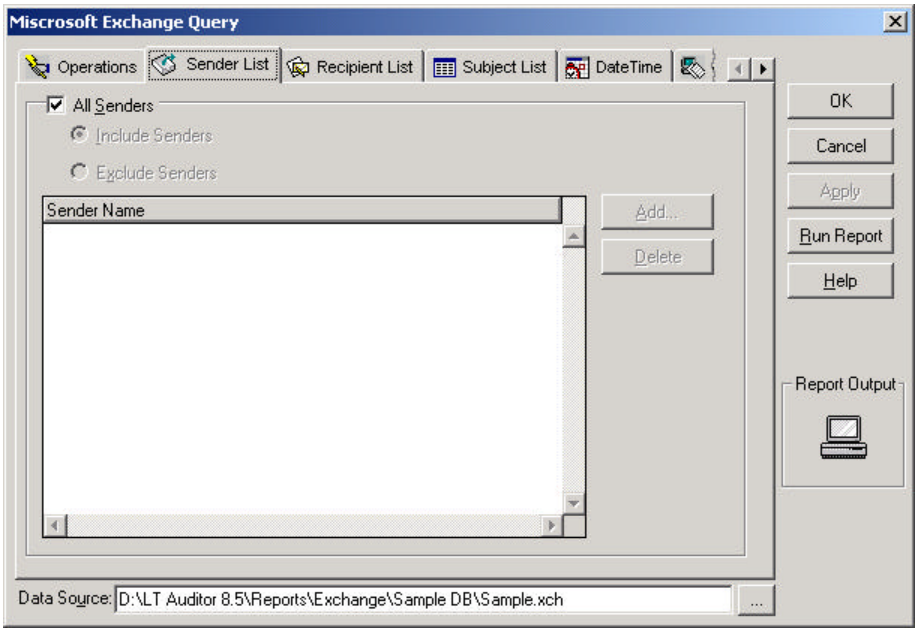
This window consists of the following tabs:

- Operations
- Sender List
- Recipient List
- Subject List
- Date & Time
- Output
- Options

Note

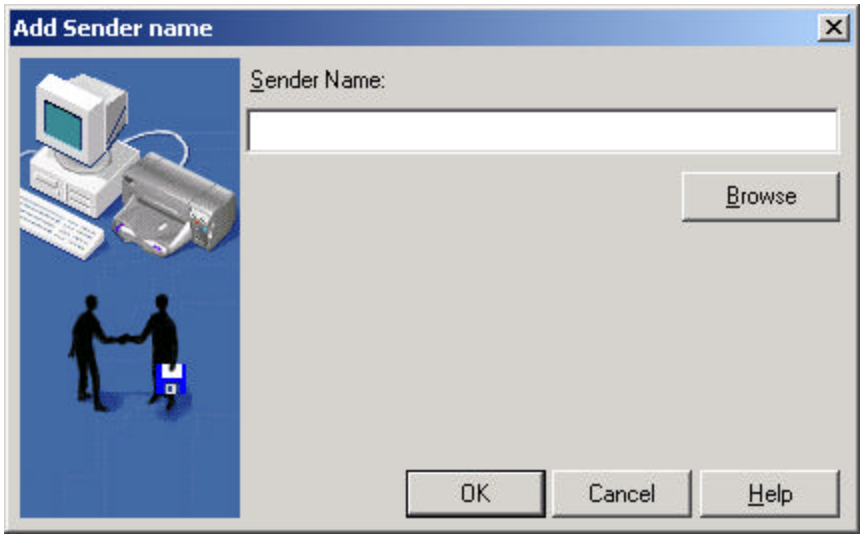
For a detailed description of using the Operations, Date & Time, Output, and Options tabs, refer to the section Cross Platform Operating System Log Query in this chapter.

Sender List Tab

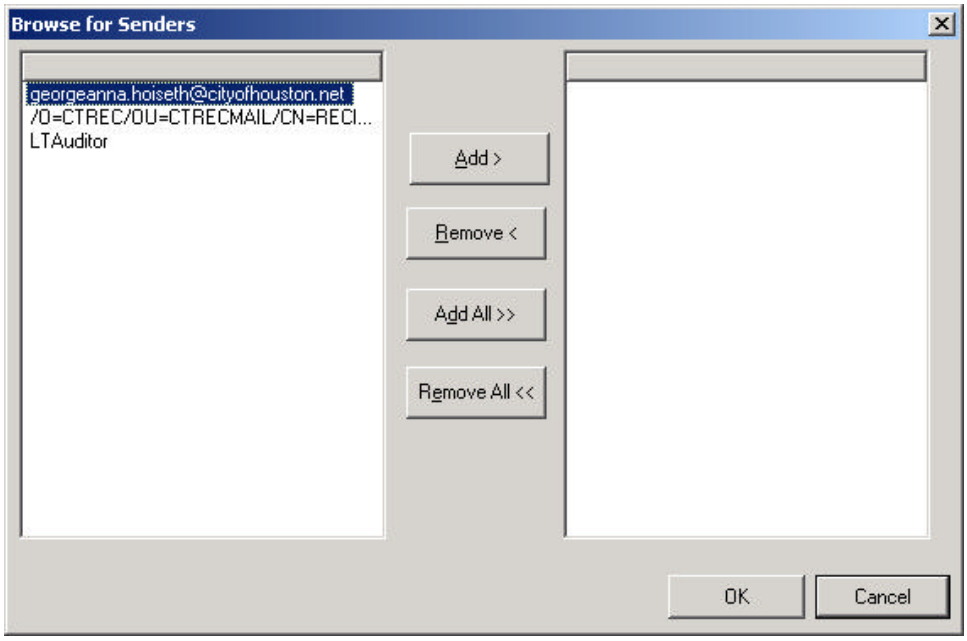


Select the Sender List tab to query specific users.

1. Check the *All Senders* box to query all users within the network, or deselect the box to query selected users.
2. Click *Include Senders* to report on selected users, or click *Exclude Senders* to report all users other than those selected in the *Sender List* tab.
3. Click *Add* to add a specific user to the query and to display the Add Sender name window.



4. Enter the name of the user you want to include in your query or click the *Browse* button. If you enter the user name, you must use the full syntax. For Windows NT, enter *domain\username.* For NetWare, enter *username.context*. Select the desired user from the list provided. If you click *Browse* the following window will display.



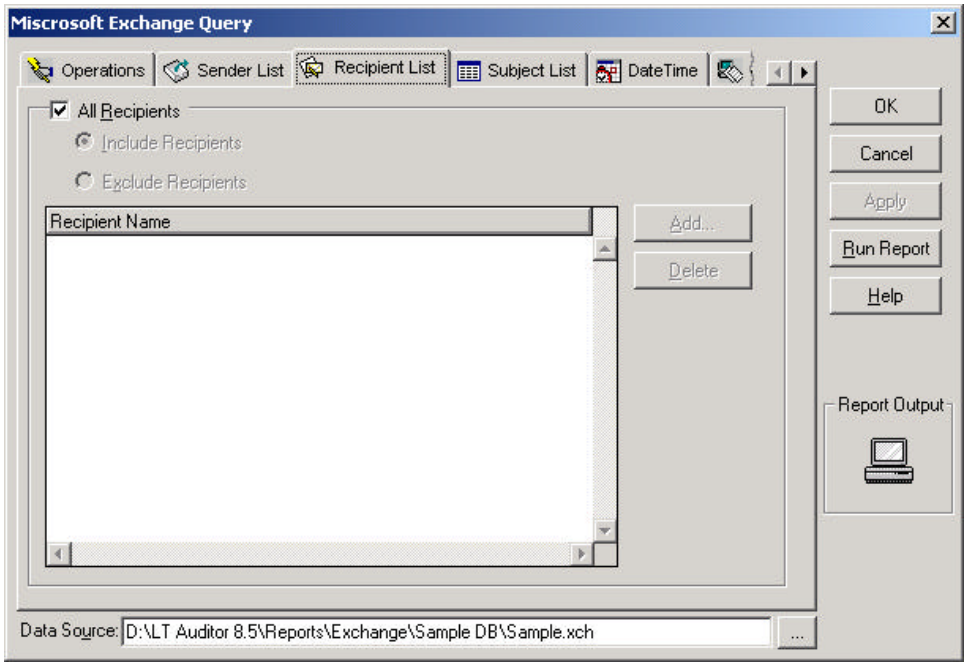
5. Select a user name and click *Add*. Click *OK* to save your changes and display the Add Sender name window.

6. Click *OK* to include the user name in your query and display the Sender List tab window.

7. Click *Delete* to remove the selected user from the query.

8. In the report query window, click the *Recipient List* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

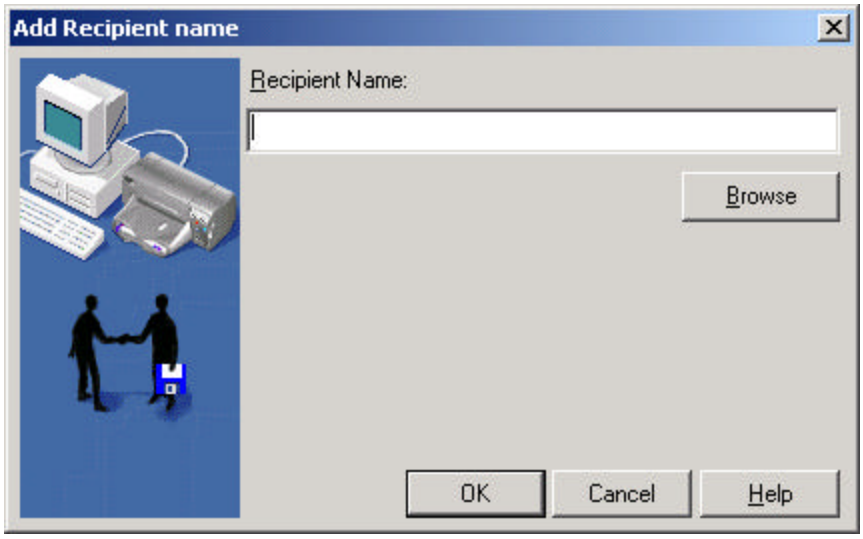
Recipient List



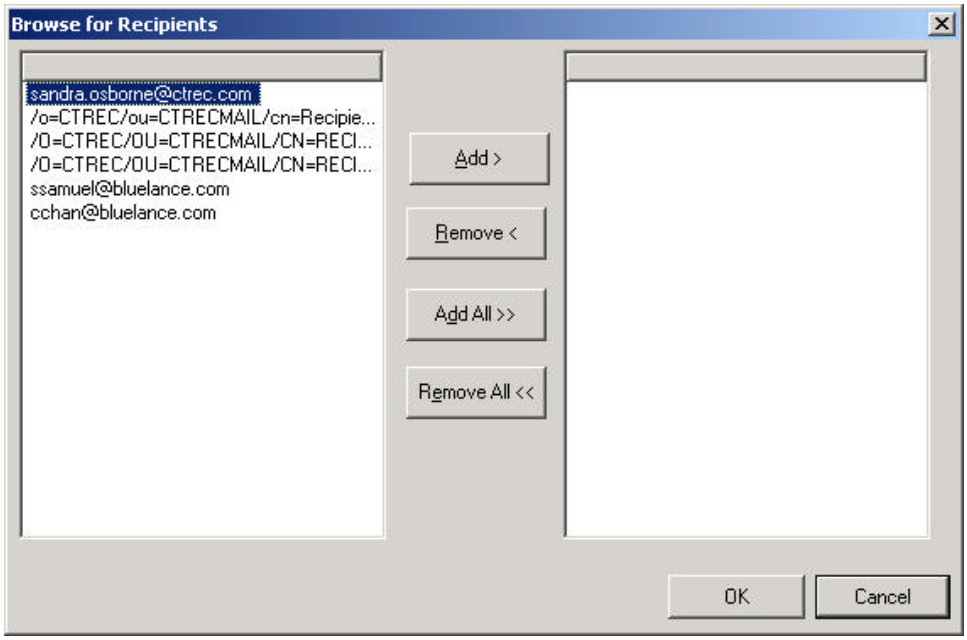
Select the Recipient List tab to query specific addressees.

1. Check the *All Recipient* box to query all users within the network, or deselect the box to query selected users.
2. Click *Include Recipients* to report on selected users, or click *Exclude Recipients* to report all users other than those selected in the *Recipient List* tab.

3. Click *Add* to add a specific user to the query and to display the Add Recipient name window.



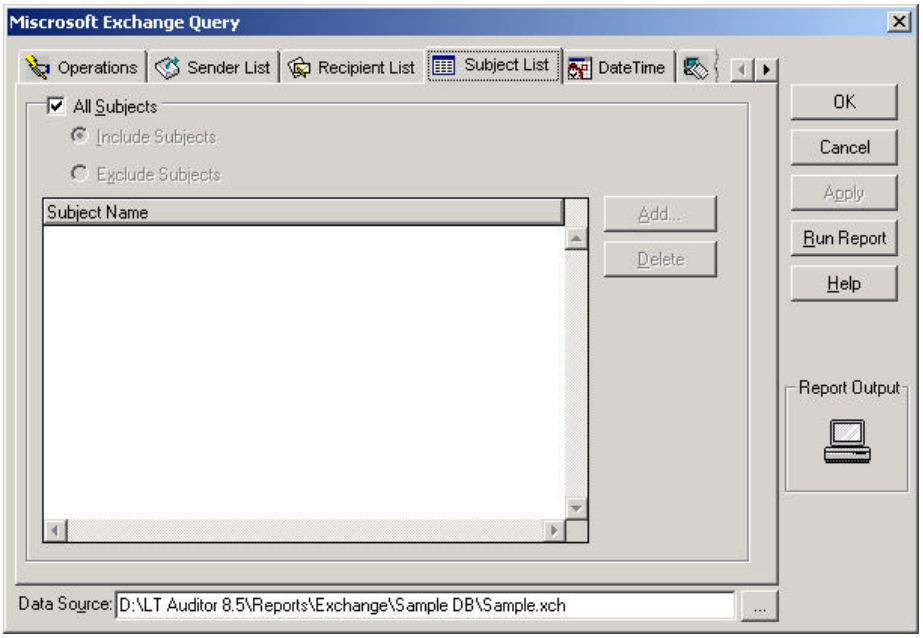
4. Enter the name of the user you want to include in your query or click the Browse button. If you enter the user name, you must use the full syntax. For Windows NT, enter domain\username. For NetWare, enter username.context. Select the desired user from the list provided. If you click *Browse* the following window will display.



5. Select a recipients name and click *Add*. Click *OK* to save your changes and display the Add Recipient name window.

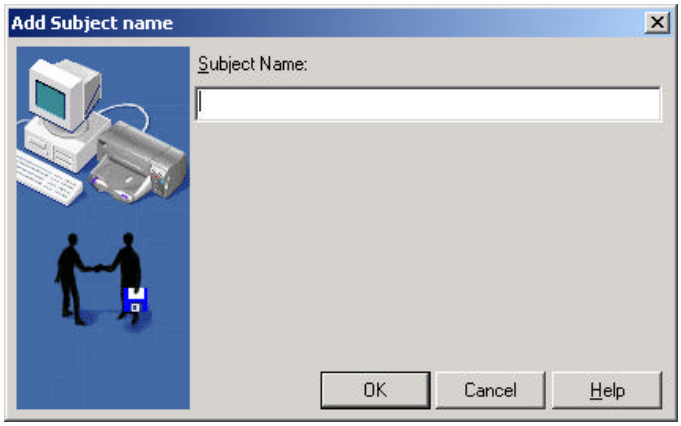
6. Click *OK* to include the user name in your query and display the Recipient List tab window.
7. Click *Delete* to remove the selected user from the query.
8. In the report query window, click the *Subject List* tab to select more criteria for your query, click *Apply* → *OK* to save your query, or click *Run Report*.

Subject List Tab



Select the Subject List tab to query specific addressees.

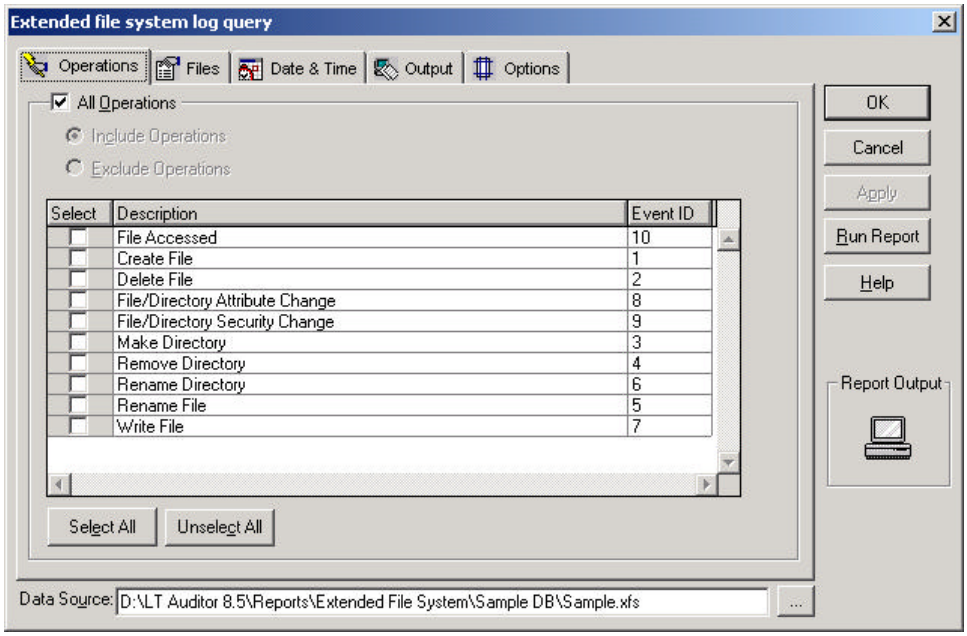
1. Check the *All Subjects* box to query all users within the network, or deselect the box to query selected subjects.
2. Click *Include Subjects* to report on selected subjects, or click *Exclude Subjects* to report all subjects other than those selected in the *Subject List* tab.
3. To enter a specific subject, click the *Add* button. The following window displays.



4. In the Subject Name field, enter a subject. Click *OK*. The newly added subject name displays in the Subject Name column.

Extended File System Log Report Query Window

If you select a query from a group in the Extended File System Logs package the following window displays.



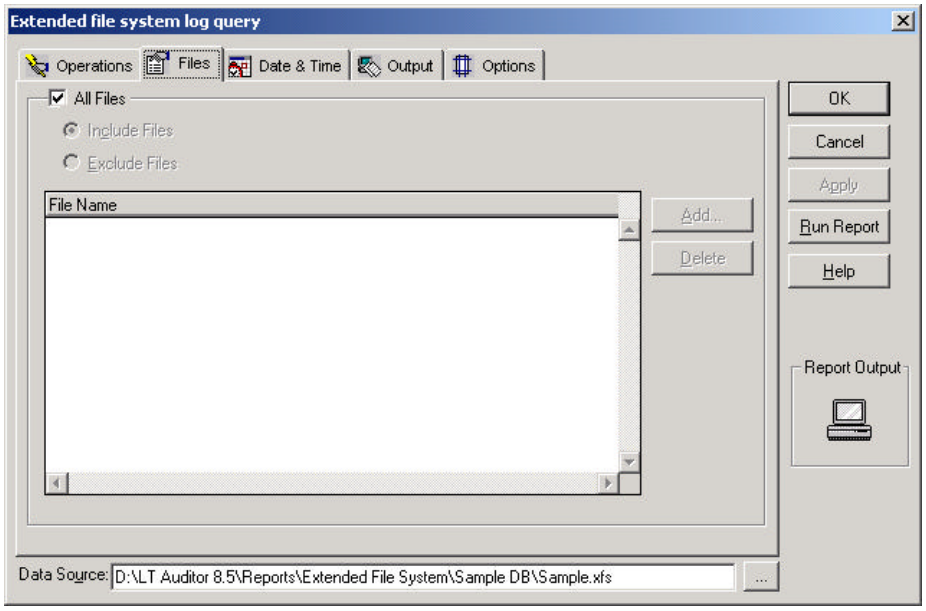
This window includes the following tabs:

- Operations
- Files
- Date & Time
- Output
- Options

Note

For a detailed description of using the Operations, Date & Time, Output, and Options tabs, refer to the section Cross Platform Operating System Log Query in this chapter.

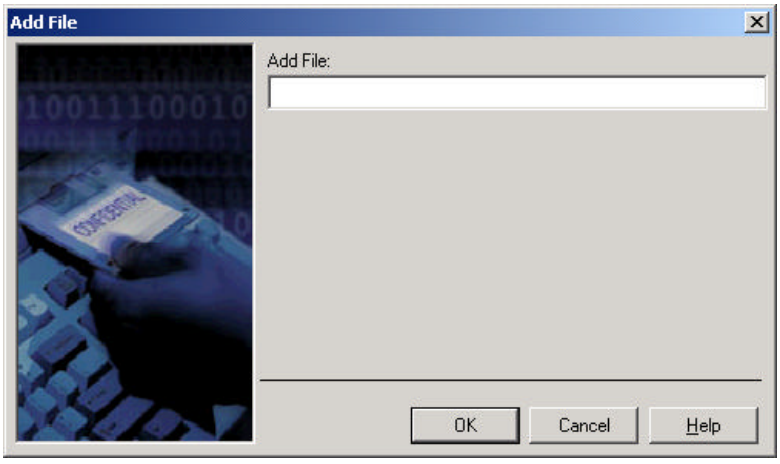
Files Tab



Using the Files tab, you can query specific files. By default, the *All Files* check box is select on all new report queries.

To modify the Files tab, perform the following steps:

1. Deselect the *Files* check box. Select *Include Files* to query all files. If you do not want to query files, select *Exclude Files*.
2. To include or exclude a specific file, click *Add*. The Add File window displays.



3. Enter the file name including its extension. For example, you can query test.chm. Click *OK*. The newly added file displays in the File Name column.

Creating a New Report Query

Perform the following steps to add a new query to the desired report group:

1. Select the report group for which you would like to add a new query.
2. To display the Report Query window, use any of the following methods:
   - From the System menu, click *New* → *Report Query*.
   - From the Standard toolbar, click the *New Report Query* button.
   - Press *Ctrl + Q.*
3. The report query window includes multiple tabs. Select a tab and modify the information according to your requirements.
4. Select the desired LT Auditor+ data source to be used for this report query.
5. Click the *Options* tab and enter a description for this query.
6. Click *Apply* → *OK* to save the query to the selected report group folder and display the report query.

Deleting a Report Query

Perform the following steps to delete a query:

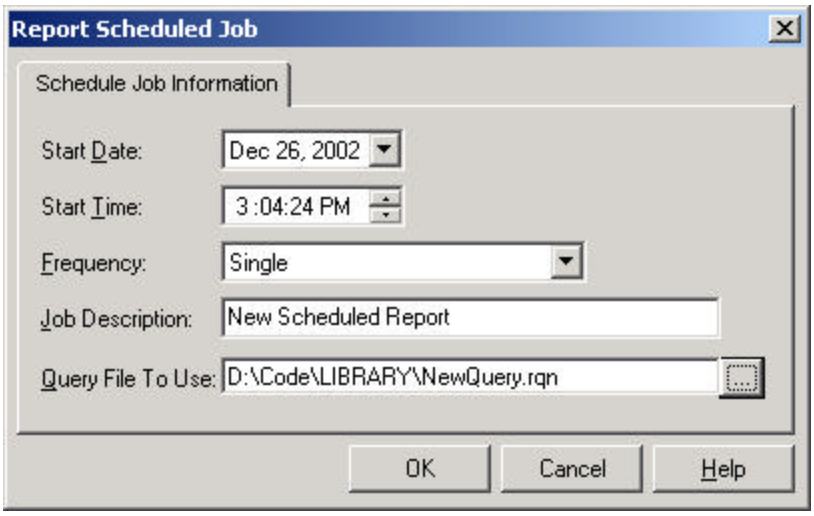
1. Highlight the desired report group corresponding to the query you want to delete. All queries in this group are displayed in the top right-hand pane.
2. Highlight the query to be deleted.
3. To delete a query, use any of the following methods:
   - From the System menu, click *Delete.*
   - From the Standard toolbar, click the *Delete* button.
4. Click *Yes* to confirm the deletion of the report query.

Copying and Pasting Queries

Perform the following steps to copy and paste a query to the desired report group:

1. Highlight the desired report group to display all queries that are part of the selected group.
2. Highlight the query to be copied.
3. From the Standard toolbar, click the *Copy* button.
4. Select the desired report group that the query is to be copied to.
5. Select the *Paste* button on the Standard toolbar. Your query is now copied to a new report group.

Scheduling Reports



A built-in scheduler enables you to schedule the LT Auditor+ reporting process on a single, daily, weekly, or monthly. Because a large quantity of data can be collected during the audit process, real-time reporting requires substantial computer and human resources. Real-time reporting can be scheduled for off-peak business periods, which frees human and computer resources during peak business hours, increasing productivity.

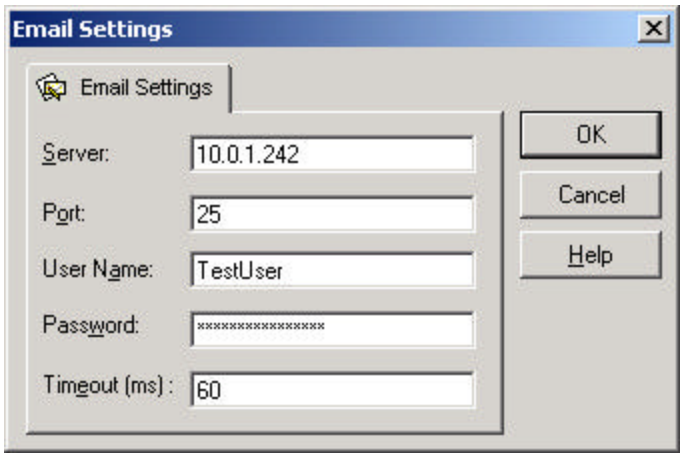
To add scheduled jobs:

1. Select a report group.
2. From the System menu, select *New* → *Scheduled Report* to display the Report Schedule Job window.
3. Enter the necessary information into each field.
    a. Start Date — Date when the job should mature for implementation
    b. Start Time — Time when the job should mature for implementation
    c. Frequency — Frequency of this job
    d. Job Description — A simple text description for this job. This field is optional
    e. Query File to Use — The data source file to use while generating the report

Additional Functions

Report Generator contains additional functions that will help you use the product efficiently.

Email Settings



Use the Email Settings window to ensure that the SMTP parameters are properly configured, so that your reports can be delivered using the e-mail option.

1. From the Options menu, click *E-mail Settings* to display the Email Settings window.
2. Enter the name or IP address of the SMTP server used within the organization. The port field includes your current settings. By default, the Timeout field is 60000 and is measured in milliseconds.

LT Auditor+ 8.0 SP2 SQL Report Generator

Appendix A — Additional Features and Modifications

This chapter provides a list of additions and changes that were made to the LT Auditor+ 8.0 SQL Report Generator.

Packages

The report groups and queries in the LT Auditor+ 8.0 SP2 Report Generator are contained within the following packages:

- **Cross Platform Operating System Logs** — Contains all of the default groups and queries shipped with LT Auditor+ 8.0 SP2 SQL Report Generator. This package can be used to query both Windows and Novell NetWare logs.
- **Microsoft Exchange Logs (Beta)** *new!* — Used to run reports on Microsoft Exchange 5.5 and Microsoft Exchange 2000 Logs.
- **Extended File System Logs** *new!* — Used to query log data collected from file system activity. The Extended File System log monitors files in the NTFS or FAT Windows File system. This package includes operations not picked up by the Windows Event Log such as File Accessed, Make Directory, and Remove Directory.
- **Microsoft Windows Logs** *new!* — *U*sed to report on Microsoft Windows logs exclusively. This package is useful when only Microsoft Windows operating system logs need to be audited.
- **Novell NetWare Logs** *new!* — Used to report on NetWare logs exclusively. This package is useful when only Novell NetWare logs need to be audited.

XML Reporting

A new and exciting feature included in LT Auditor+ 8.0 SP2 SQL Report Generator is XML reporting. This feature allows a user to directly run a report on an XML based log file. Use this option when a report needs to be generated on a specific file. The following packages can report on XML logs with the .xml extension.

- Cross Platform Operating System logs
- Microsoft Windows logs
- Novell NetWare logs

The Microsoft Exchange logs (Beta) package can report on XML files with an .xch extension. The Extended File System Logs package can report on XML files with an ".xfs" extension.
To run a report on an xml log file, select the appropriate XML file as the data source for that query.

Additional Features and Modifications

The following features have been added to the LT Auditor+ SQL Report Generator:

- The data source window allows you to test the connection to an Oracle or a SQL server database. This feature prevents errors that may occur from invalid or erroneous connection settings.
- The License key can be changed from the Report Generator window by clicking *Help → About LT Auditor+ Report Generator→ License*. For further information on license keys, contact the Blue Lance Support team at (713) 680-1187 or the Blue Lance website at http://www.bluelance.com.

The following modification has been made to the LT Auditor+ SQL Report Generator:

- Copying and pasting queries across different packages is not allowed. If you attempt to perform this action, a warning message will display.